

Hefez, Abramo

Curso de Álgebra, volume 1 (3^a edição).

Associação Instituto Nacional de Matemática Pura e
Aplicada, Rio de Janeiro, 2002

226 pp. (Coleção Matemática Universitária)

Bibliografia

1. Álgebra. 2. Teoria dos Números. I. Título. II. Série.

CDD-512

Curso de Álgebra

Volume 1

Terceira Edição

Abramo Hefez



INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

Copyright © 2002 by Abramo Hefez
Direitos reservados, 2002 pela Associação Instituto
Nacional de Matemática Pura e Aplicada - IMPA
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ

Impresso no Brasil / Printed in Brazil

Capa: Rodolfo Capeto e Noni Geiger.

Coleção Matemática Universitária

Comissão Editorial:

Elon Lages Lima (Editor)
S. Collier Coutinho
Alfredo Iusem

Títulos Publicados:

- Análise Real, Volume 1 – Elon Lages Lima
- EDP: Um Curso de Graduação – Valéria Iório
- Curso de Álgebra, Volume 1 – Abramo Hefez
- Álgebra Linear – Elon Lages Lima
- Introdução às Curvas Algébricas Planas – Israel Vainsencher
- Equações Diferenciais Aplicadas – Djairo G. de Figueiredo e Aloisio Freiria Neves
- Geometria Diferencial – Paulo Ventura Araújo
- Introdução à Teoria dos Números – José Plínio de Oliveira Santos
- Cálculo em Uma Variável Complexa – Marcio G. Soares
- Geometria Analítica e Álgebra Linear – Elon Lages Lima
- Números Primos: Mistérios e Recordes – Paulo Ribenboim

Distribuição:

IMPA
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ
e-mail: dic@impa.br
<http://www.impa.br>

ISBN: 85-244-0079-X

Prefácio

Este livro teve como origem as notas de aula de um Curso de Álgebra de três semestres que ministrei várias vezes ao longo de mais de uma década na Universidade Federal do Espírito Santo. Trata-se do primeiro de dois volumes de um curso completo de Álgebra para alunos de graduação em Matemática e cursos afins. A boa acolhida dada às notas de aula por parte dos alunos e colegas, além do convite e o estímulo que recebi do diretor desta coleção, Professor Elon Lages Lima, muito me motivaram a escrever este livro.

A estrutura global do curso é a seguinte. No primeiro semestre são apresentados os números inteiros, os números racionais e as estruturas de anéis e corpos, dando ênfase às propriedades dos domínios principais e explorando a relação entre Álgebra e Aritmética. No segundo semestre são estudados os números complexos, os anéis de polinômios e as equações do 3º e 4º graus pelos métodos clássicos e de Lagrange, introduzindo os grupos de permutações. O terceiro semestre é dedicado à teoria das equações segundo Galois e ao estudo dos grupos finitos.

Os capítulos de números reais e de inteiros gaussianos, na realidade não constavam dos cursos ministrados e foram escritos e incorporados ao texto com a finalidade de completá-lo. Estes capítulos podem ser cobertos sob forma de seminários com os alunos.

A seguir é apresentada uma sugestão para a utilização deste livro. O Capítulo 1 serve apenas para fixar as notações e introduzir os fatos básicos sobre conjuntos e funções. Para o primeiro curso de um semestre de duração sugere-se a utilização dos Capítulos 2 a 7. O Capítulo 9 juntamente com os capítulos iniciais do segundo volume constituem o segundo curso.

Este livro deve a sua existência a várias pessoas a quem gostaria de transmitir os meus profundos agradecimentos.

Aos colegas e alunos do Departamento de Matemática da UFES que durante todos estes anos usaram o material que deu origem ao livro. À Maria Lúcia Campos, Moacir Rosado Filho e Valmecir Bayer por suas sugestões e críticas às notas de aula e exercícios. Ao colega Luiz Manoel de Figueiredo pela leitura crítica e às sugestões dadas durante a elaboração do texto final. Ao Elon Lages Lima pela amizade e pelo continuado estímulo para escrever este livro. À Fundação Vitae pelo oportuno patrocínio. Ao Luiz Alberto da S. Santos pelo excelente trabalho de datilografia. À Graftex pelo primoroso trabalho de composição e fotolito digital.

Rio de Janeiro, 14 de abril de 1993.

Abramo Hefez

Prefácio à segunda edição

Nesta segunda edição nos limitamos a corrigir alguns erros tipográficos. Agradecemos a todos que nos mandaram as suas observações.

A confirmação da exatidão da prova de A. Wiles do Último Teorema de Fermat nos fez retirar o apêndice que lhe dedicamos na primeira edição para inserir um comentário no lugar apropriado do texto.

Rio de Janeiro, 14 de junho de 1997.

Abramo Hefez

Conteúdo

Capítulo 1. A Linguagem dos Conjuntos	1
1. Conjuntos	1
2. Operações com Conjuntos	6
3. Funções	12
4. Funções Bijetoras e Funções Inversas	17
Capítulo 2. Os Números Inteiros e Racionais	22
1. Os Números Inteiros	23
2. Os Números Racionais	35
Capítulo 3. Propriedades dos Inteiros	42
1. Indução Matemática	42
2. Divisão com Resto	56
3. Sistemas de Numeração	60
4. Euclides	64
Capítulo 4. A Álgebra dos Inteiros	66
1. Divisibilidade	66
2. Ideais	72
3. Fatoração	77
Capítulo 5. A Aritmética dos Inteiros	87
1. Números Primos	88
2. Sobre a Distribuição dos Números Primos	93
3. Algoritmo de Euclides	95
4. Equações Diofantinas	101
5. O Despertar da Aritmética	105
Capítulo 6. Congruências	107
1. Propriedades das Congruências	107
2. As Classes Residuais e a sua Aritmética	116
3. Congruências Lineares	123
4. A Função Φ de Euler	127
5. O Legado de um Gigante	129
Capítulo 7. Anéis	132
1. Anéis	132
2. Homomorfismo e Ideais	136
3. Anéis Quocientes	141

Capítulo 8. Os Números Reais	148
1. Seqüências Convergentes	149
2. Corpos Arquimedianos	154
3. Seqüências Fundamentais	159
4. Ordenação do Completamento	166
5. Relação com a Análise	173
Capítulo 9. Os Números Complexos	177
1. O Corpo dos Números Complexos	178
2. Conjugação e Módulo	184
3. Forma Trigonométrica dos Números Complexos	186
4. Raízes de Números Complexos	189
5. Raízes da Unidade	192
Capítulo 10. Os Inteiros Gaussianos	198
1. O Anel dos Inteiros Gaussianos	198
2. Elementos Primos de $\mathbb{Z}[i]$	204
3. A Equação Pitagórica	210
4. Quocientes do Anel dos Inteiros Gaussianos	212
5. O Exemplo de Kummer	218
Bibliografia	222
Índice	223

A Linguagem dos Conjuntos

A Teoria dos Conjuntos foi criada no final do século 19 por Georg Cantor para abordar certas questões matemáticas. As idéias de Cantor, de início muito combatidas, foram rapidamente se impondo como elemento unificador dos vários ramos da matemática, tornando-se o meio pelo qual é formalizada toda a matemática contemporânea.

O nosso tratamento para a Teoria dos Conjuntos será deliberadamente ingênuo, não nos preocupando portanto em fundamentá-lo com rigor.

1. Conjuntos

Os termos *conjunto* e *elemento* e a relação de um elemento pertencer a um conjunto são conceitos que não procuraremos definir.

Usa-se o termo *coleção* como sinônimo de conjunto. Os conjuntos são usualmente designados por letras maiúsculas enquanto que os elementos o são por letras minúsculas. A afirmação de que o elemento a pertence ao conjunto A é simbolizada por

$$a \in A,$$

enquanto que a sua negação é simbolizada por

$$a \notin A.$$

Dois conjuntos são *iguais* se eles tem os mesmos elementos. Mais precisamente, temos que $A = B$ se e somente se todo elemento de A é elemento de B e todo elemento de B é elemento de A .

A condição de que todo elemento de um conjunto A pertence a um

conjunto B estabelece uma relação entre A e B chamada de relação de *inclusão*. Quando existir uma tal relação entre A e B escreveremos

$$A \subset B \quad \text{ou} \quad B \supset A,$$

que se lê A está *contido* em B, ou A é *subconjunto* de B, ou ainda B *contém* A.

A relação de inclusão possui claramente as seguintes propriedades

- 1) $A \subset A$, para todo conjunto A
- 2) $A = B$ se e somente se $A \subset B$ e $B \subset A$
- 3) Se $A \subset B$ e $B \subset C$, então $A \subset C$.

A negação de $A \subset B$ é simbolizada por $A \not\subset B$. Para mostrar que $A \not\subset B$ deve-se exibir pelo menos um elemento de A que não pertence a B. Se $A \subset B$ e $A \neq B$, diremos que A é *subconjunto próprio* de B. Neste caso, escrevemos

$$A \subsetneq B.$$

No que segue admitiremos o leitor familiarizado com o conjunto \mathbb{N} dos *números naturais* cujos elementos são os números

$$1, 2, 3, \dots$$

e com o conjunto \mathbb{Z} dos *números inteiros*

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

Um conjunto pode ser dado exibindo-se todos os seus elementos. Por exemplo, $\{a, b, c\}$ é o conjunto formado pelas três primeiras letras do nosso alfabeto, o conjunto $\{1\}$ é formado por apenas um elemento que é o número 1. Quando não houver risco de confusão, poderemos dar, por exemplo, um conjunto do seguinte modo

$$\{1, 2, 3, \dots, 1000\},$$

onde as reticências subentendem os inteiros de 4 a 999.

No que segue mostraremos como construir novos conjuntos a partir de conjuntos dados. Antes porém, introduziremos a noção importante de sentença aberta.

Diremos que x é uma *indeterminada* para o conjunto A se x é uma letra que não figura em A .

Uma *sentença aberta* $P(x)$ em um conjunto A é uma sentença que contém uma indeterminada x para A tal que toda vez que se substitui x por um elemento a de A , obtém-se uma sentença $P(a)$ que é verdadeira ou falsa.

Exemplos

a. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta

$$x \geq 0.$$

É claro que ao substituir x por um número inteiro, obtemos uma sentença que é verdadeira ou falsa. Em particular, são verdadeiras $P(0)$, $P(1)$ e $P(8)$, enquanto que são falsas $P(-1)$, $P(-2)$ e $P(-8)$.

b. Sejam A um conjunto qualquer e $P(x)$ a sentença aberta,

$$x \in A.$$

É claro que $P(a)$ é verdadeira para todo $a \in A$.

c. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta,

$$\text{Existe } n \in \mathbb{Z} \text{ tal que } x = 2 \cdot n.$$

Temos que $P(0)$, $P(2)$ e $P(-4)$ são verdadeiras enquanto que $P(1)$ e $P(-1)$ são falsas. É claro que $P(a)$ é verdadeira se e somente se a é um número par.

d. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta,

$$\text{Existem } m \text{ e } n \text{ inteiros tais que } x = m \cdot 4 + n \cdot 6.$$

Temos que $P(2)$ é verdadeira pois $2 = 2 \cdot 4 + (-1) \cdot 6$ ($m = 2$ e $n = -1$); $P(-6)$ é verdadeira ($m = 0$ e $n = -1$); $P(0)$ é verdadeira ($m = n = 0$); $P(3)$ é falsa (justifique).

e. Sejam A um conjunto e $P(x)$ uma sentença aberta em A . Formase uma nova sentença aberta em A tomando a negação (não $P(x)$) de $P(x)$. Temos que (não $P(a)$) é verdadeira se e somente se $P(a)$ é falsa.

Por exemplo, se $A = \mathbb{Z}$ e $P(x)$ é a sentença aberta $x < 0$, então (não $P(x)$) é a sentença aberta $x \geq 0$.

f. Sejam A um conjunto e $P(x)$ a sentença aberta em A ,

$$x \neq x.$$

Temos que $P(a)$ é falsa para todo $a \in A$.

Como o conceito de conjunto não foi definido, não será possível provar a existência de certos conjuntos. Isto terá que ser estabelecido caso a caso por meio de um axioma específico, como faremos a seguir.

Dados um conjunto A e uma sentença aberta $P(x)$ em A admitiremos a existência de um subconjunto de A formado pelos elementos a de A para os quais $P(a)$ é verdadeira. Este conjunto será denotado por

$$\{x \in A \mid P(x)\}.$$

Exemplos

a'. O conjunto $\{x \in \mathbb{Z} \mid x \geq 0\}$ é o conjunto de todos os números inteiros não negativos. Este conjunto será denotado por \mathbb{Z}^+ . Denotaremos por \mathbb{Z}^- o conjunto inteiros não positivos.

b'. Temos que $\{x \in A \mid x \in A\} = A$

c'. Temos que $\{x \in \mathbb{Z} \mid \text{existe } n \in \mathbb{Z} \text{ tal que } x = 2 \cdot n\}$ é o conjunto dos números inteiros pares.

d'. Os conjuntos do tipo $\{x \in \mathbb{Z} \mid \text{existem } n \text{ e } m \text{ inteiros tais que } x = m \cdot 4 + n \cdot 6\}$ serão estudados detalhadamente no Capítulo 4.

e'. Seja $P(x)$ uma sentença aberta num conjunto A . Considere os conjuntos $B = \{x \in A \mid P(x)\}$ e $B' = \{x \in A \mid (\text{não } P(x))\}$. É claro que B e B' não tem elementos em comum e que qualquer elemento de A pertence a um destes dois conjuntos.

f'. O conjunto $\{x \in A \mid x \neq x\}$ não tem nenhum elemento.

O último exemplo acima nos conduz a admitir a existência de um conjunto que não tem elementos. Tal conjunto será chamado de *conjunto vazio* e será simbolizado por \emptyset .

Afirmamos que $\emptyset \subset A$ qualquer que seja o conjunto A . Esta afirmação parece estranha à primeira vista, mas veja como é natural a falsidade de sua negação (isto é, a sua veracidade). A afirmação $\emptyset \not\subset A$ significa que existe $x \in \emptyset$ tal que $x \notin A$ e isto é claramente falso visto que o conjunto \emptyset não possui nenhum elemento.

No decorrer do texto usaremos as seguintes notações e regras da lógica simbólica.

Sejam $P(x)$ uma sentença aberta e A um conjunto. Usaremos as notações

$$\forall x \in A, \quad P(x),$$

para representar a sentença, *para todo x em A , a asserção $P(x)$ é verdadeira*, e

$$\exists x \in A \mid P(x)$$

para representar a sentença, *existe x em A tal que $P(x)$ é verdadeira*.

A negação da sentença $\forall x \in A, P(x)$ é a sentença

$$\exists x \in A \mid (\text{não } P(x)),$$

enquanto que a negação da sentença $\exists x \in A \mid P(x)$ é a sentença

$$\forall x \in A, (\text{não } P(x)).$$

Usaremos os conectivos *e* e *ou*, sendo que o conectivo *ou* terá sentido inclusivo, isto é significando uma coisa ou outra, ou ambas. Se P e Q são sentenças, a negação de P ou Q é

$$(\text{não } P) \quad e \quad (\text{não } Q),$$

enquanto que a negação de P e Q é

$$(\text{não } P) \quad ou \quad (\text{não } Q).$$

Problemas

1.1 Falso ou verdadeiro:

- | | |
|-------------------------------------|---------------------------------------|
| a) $\{a, a, b, c\} = \{a, b, c\}$ | b) $\{a\} = \{a, \{a\}\}$ |
| c) $\{a\} \in \{a, \{a\}\}$ | d) $\{a\} \subset \{a, \{a\}\}$ |
| e) $\{\{a\}\} \subset \{a, \{a\}\}$ | f) $\{a, b\} \subset \{a, \{a, b\}\}$ |

1.2 Falso ou verdadeiro:

- a) $\emptyset \in \{\emptyset\}$ b) $\emptyset = \{\emptyset\}$ c) $\emptyset \subset \{\emptyset\}$
 d) $\{\emptyset\} \subset \{\{\emptyset\}\}$ e) $\{\emptyset\} \in \{\{\emptyset\}\}$ f) $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$

1.3 Quantos subconjuntos tem cada um dos seguintes conjuntos

- a) {1} b) {1, 2} c) {1, 2, 3}

Generalize.

1.4 Caracterize todos os inteiros x para os quais é verdadeira a sentença aberta $P(x)$ dada por

- a) Existem inteiros m e n tais que $x = m \cdot 2 + n \cdot 3$
b) Existem inteiros m e n tais que $x = m \cdot 4 + n \cdot 6$

2. Operações com Conjuntos

2.1. União de Conjuntos

Dada uma coleção qualquer de conjuntos, admitiremos a existência de um conjunto cujos elementos pertencem a pelo menos um dos conjuntos da coleção. Tal conjunto será chamado de *união* dos conjuntos da coleção.

Dados dois conjuntos A e B, a sua união é portanto o conjunto de todos os elementos que pertencem a A ou pertencem a B, que será denotada por $A \cup B$:

Por exemplo, se $A = \{a, b, c\}$ e $B = \{b, c, d\}$, então $A \cup B = \{a, b, c, d\}$.

Quando numa discussão usarmos uma “sentença aberta” $P(x)$ sem especificar sobre que conjunto ela é definida, subentende-se que é definida sobre a união de todos os conjuntos que intervém na discussão.

As seguintes propriedades seguem imediatamente das definições.

Propriedades: Para todos os conjuntos A , B e C temos que

- 1) $A \cup \emptyset = A$ e $A \cup A = A$
- 2) $A \subset A \cup B$ e $B \subset A \cup B$
- 3) $A \cup B = B \cup A$
- 4) $(A \cup B) \cup C = A \cup (B \cup C)$

Proposição 1. *Dados conjuntos A, A', B e B' com $A \subset B$ e $A' \subset B'$, então $A \cup A' \subset B \cup B'$.*

Demonstração: Se $A \cup A' = \emptyset$, a asserção é claramente verdadeira. Suponha que $A \cup A' \neq \emptyset$. Se $x \in A \cup A'$, temos que $x \in A$ ou $x \in A'$ e como $A \subset B$ e $A' \subset B'$, segue que $x \in B$ ou $x \in B'$, logo $x \in B \cup B'$. Isto prova que $A \cup A' \subset B \cup B'$. \square

Corolário. $A \cup B = A$ se e somente se $B \subset A$.

Demonstração: Suponhamos que $A \cup B = A$. Como $B \subset A \cup B$, segue que $B \subset A$.

Reciprocamente, suponha que $B \subset A$. Como $A \subset A$, segue pela proposição que $A \cup B \subset A \cup A = A$, logo $A \cup B \subset A$. Como $A \subset A \cup B$, segue que $A \cup B = A$. \square

2.2. Interseção de Conjuntos

Dados dois conjuntos A e B , a *interseção* de A e B é o conjunto

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}.$$

Quando $A \cap B = \emptyset$, dizemos que os conjuntos A e B são *disjuntos*.

Por exemplo, se $A = \{a, b, c\}$, $B = \{b, c, d\}$ e $C = \{d, e, f\}$, então $A \cap B = \{b, c\}$ e A e C são disjuntos.

As seguintes propriedades decorrem imediatamente das definições

Propriedades: Para todos os conjuntos A, B e C temos que

- 1) $A \cap \emptyset = \emptyset$ e $A \cap A = A$
- 2) $A \cap B \subset A$ e $A \cap B \subset B$
- 3) $A \cap B = B \cap A$

$$4) \quad (A \cap B) \cap C = A \cap (B \cap C)$$

Proposição 2. *Dados conjuntos A, B e C quaisquer, temos que*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Demonstração: Inicialmente provaremos a inclusão

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C).$$

Se $A \cap (B \cup C) = \emptyset$, nada temos a provar. Suponha que $A \cap (B \cup C) \neq \emptyset$. Seja x um elemento qualquer de $A \cap (B \cup C)$. Logo $x \in A$ e $x \in B \cup C$. Se $x \in B$, então $x \in A \cap B$. Se $x \in C$, então $x \in A \cap C$. Em qualquer caso temos que $x \in (A \cap B) \cup (A \cap C)$.

Agora provaremos a inclusão

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C).$$

Se o conjunto da esquerda for vazio, a inclusão é obviamente verificada. Suponha agora que tal conjunto é não vazio e seja x um elemento qualquer dele. Logo $x \in A \cap B$ ou $x \in A \cap C$. Em qualquer caso $x \in A$ e temos que $x \in B$ ou $x \in C$. Portanto $x \in A \cap (B \cup C)$. \square

Proposição 3. *Dados conjuntos A, B e C quaisquer, temos que*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demonstração: Deixamos esta demonstração a cargo do leitor. \square

2.3. Diferença de Conjuntos

Dados dois conjuntos A e B, a diferença A menos B é o conjunto

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}.$$

Quando $B \subset A$, a diferença $A \setminus B$ é denotada por $C_A(B)$ e é chamada de *complementar* de B em A.

Por exemplo, se $A = \{a, b, c\}$ e $B = \{b, c, d\}$, então $A \setminus B = \{a\}$.

As seguintes propriedades decorrem imediatamente das definições.

Propriedades Para todos os conjuntos A e B , temos que

- 1) $A \setminus \emptyset = A$ e $A \setminus A = \emptyset$
- 2) Se $A \cap B = \emptyset$, então $A \setminus B = A$ e $B \setminus A = B$
- 3) $C_A(\emptyset) = A$ e $C_A(A) = \emptyset$.

Proposição 4. Sejam B e B' subconjuntos de A . Se $B \subset B'$, então

$$C_A(B') \subset C_A(B).$$

Demonstração: Suponha que $B \subset B'$ e seja x um elemento qualquer de $C_A(B')$. Logo $x \notin B'$. Segue que $x \notin B$ pois caso contrário, como $B \subset B'$ teríamos $x \in B'$. Consequentemente $x \in C_A(B)$. \square

Proposição 5. Sejam B e B' subconjuntos de A . Temos que

$$C_A(B \cup B') = C_A(B) \cap C_A(B').$$

Demonstração: A proposição segue da seguinte cadeia de equivalências:

$$\begin{aligned} x \in C_A(B \cup B') &\Leftrightarrow x \notin B \cup B' \\ &\Leftrightarrow x \notin B \quad \text{e} \quad x \notin B' \\ &\Leftrightarrow x \in C_A(B) \cap C_A(B'), \end{aligned}$$

para todo elemento x de A . \square

Proposição 6. Sejam B e B' subconjuntos de A . Temos que

$$C_A(B \cap B') = C_A(B) \cup C_A(B').$$

Demonstração: Deixada a cargo do leitor. \square

2.4. Conjuntos das Partes e Produto Cartesiano

Dado um conjunto A qualquer admitiremos a existência de um conjunto $\mathcal{P}(A)$ cujos elementos são todos os subconjuntos de A .

Um *par ordenado* (a, b) de elementos de A é um elemento de $\mathcal{P}(\mathcal{P}(A))$ da forma

$$\{\{a\}, \{a, b\}\}.$$

Não é difícil se convencer que $(a, b) = (a', b')$ se e somente se $a = a'$ e $b = b'$.

Dados dois conjuntos A e B , o *produto cartesiano* de A e B é o conjunto $A \times B$ de todos os pares ordenados (a, b) de elementos de $A \cup B$ tais que $a \in A$ e $b \in B$. Simbolicamente escrevemos

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}.$$

Por exemplo, se $A = \{a, b\}$ e $B = \{c, d\}$, temos que

$$A \times B = \{(a, c), (a, d), (b, c), (b, d)\},$$

e

$$B \times A = \{(c, a), (c, b), (d, a), (d, b)\}.$$

Note que em geral temos que $A \times B \neq B \times A$. Temos também que $A \times B = \emptyset$ se e somente se $A = \emptyset$ ou $B = \emptyset$.

2.5. Famílias de Conjuntos

Seja I um conjunto não vazio qualquer. Uma *família indexada* por I é uma coleção de conjuntos A_i com $i \in I$. Uma tal família será denotada por $(A_i)_{i \in I}$.

A união dos elementos da família é

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ para algum } i \in I\}$$

e a sua interseção é

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ para todo } i \in I\}.$$

É claro que para todo $j \in I$, temos que

$$A_j \subset \bigcup_{i \in I} A_i \quad \text{e} \quad \bigcap_{i \in I} A_i \subset A_j.$$

Problemas

2.1 Determine os seguintes conjuntos:

- a) $\mathbb{Z}^+ \setminus \mathbb{Z}^-$ b) $\mathbb{Z}^+ \cap \mathbb{Z}^-$ c) $\mathbb{Z}^+ \cup \mathbb{Z}^-$

2.2 Mostre que

- a) Se $A \subset B$ e $A' \subset B'$, então $A \cap A' \subset B \cap B'$
- b) $A \cap B = A$ se e somente se $A \subset B$

2.3 Demonstre a Proposição 3.**2.4 Mostre que se $B \subset A$, então**

- a) $B \cup C_A(B) = A$
- b) $B \cap C_A(B) = \emptyset$

2.5 Suponha que B e B' são subconjuntos de A . Mostre que

- a) $C_A(C_A(B)) = B$
- b) Se $C_A(B') \subset C_A(B)$, então $B \subset B'$
- c) $C_A(B \cap B') = C_A(B) \cup C_A(B')$

2.6 Dados B e B' subconjuntos de A , mostre que

- a) $B \cup (C_A(B) \cap B') = B \cup B'$
- b) $B \cap (C_A(B) \cup B') = B \cap B'$
- c) $B \setminus B' = C_A(B') \setminus C_A(B)$
- d) $B \setminus B' = B \cap C_A(B')$

2.7 Mostre que para quaisquer conjuntos A , B e C , vale:

- a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- c) $A \cap (B \setminus C) = (A \cap B) \setminus C$
- d) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

2.8 Suponha que $A \cap B = \emptyset$. Mostre que

- a) $A \cap (B \cup C) = A \cap C$
- b) $A \setminus B = A$
- c) $A = (A \cup B) \setminus B$

2.9 Diga se cada uma das seguintes asserções é falsa ou verdadeira. Prove-a quando verdadeira e dê um contra-exemplo quando falsa.

- $A \cup B = A \cup C \implies B = C$
- $A \cap B = A \cap C \implies B = C$
- $A \cup B = A \cup C \text{ e } A \cap B = A \cap C \implies B = C$

2.10 Demonstre as seguintes igualdades:

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) = (A \times D) \cap (C \times B)$
- $(A \times B) \setminus (C \times D) = [(A \setminus C) \times B] \cup [A \times (B \setminus D)]$

2.11 Sejam A, B, C e D conjuntos tais que $A \neq \emptyset$ e $B \neq \emptyset$. Mostre que $A \subset B$ e $C \subset D$ se e somente se $A \times C \subset B \times D$.

2.12 Sejam $(A_i)_{i \in I}$ uma família de conjuntos e A um conjunto. Mostre que

- $A \cap \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} (A \cap A_i)$
- $A \cup \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} (A \cup A_i)$
- $A \setminus \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} (A \setminus A_i)$
- $A \setminus \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} (A \setminus A_i)$

3. Funções

3.1. O Conceito de Função

Uma *função* consiste de dois conjuntos não vazios X e Y e de uma lei f que a cada elemento $x \in X$, associa um único elemento $f(x) \in Y$.

Uma função será simbolizada por

$$\begin{array}{ccc} f: X & \longrightarrow & Y \\ x & \longmapsto & f(x) \end{array}$$

Para abreviar, quando não quizermos explicitar a lei f , usaremos a notação $f: X \rightarrow Y$ e nos referiremos a f , como sendo a função.

O conjunto X é chamado de *domínio* da função f e $f(x)$ de *imagem* de x por f . Usaremos também os nomes *aplicação* ou *correspondência* como sinônimos de função.

Quando é dada uma lei $x \mapsto f(x)$ que associa aos elementos de X elementos de Y , para termos certeza que esta lei define uma função $f: X \rightarrow Y$, devemos verificar que efetivamente a cada elemento de X é associado um único elemento de Y . Deve-se então mostrar que se $a = b$, então $f(a) = f(b)$.

Duas funções

$$\begin{array}{ccc} f_1: X_1 & \longrightarrow & Y_1 \\ x & \longmapsto & f_1(x) \end{array}, \quad \begin{array}{ccc} f_2: X_2 & \longrightarrow & Y_2 \\ x & \longmapsto & f_2(x) \end{array}$$

serão considerados *iguais*, escrevendo neste caso $f_1 = f_2$, se $X_1 = X_2$, $Y_1 = Y_2$ e $f_1(x) = f_2(x)$ para todo $x \in X_1 = X_2$.

Exemplos

1. Seja

$$\begin{array}{ccc} f: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x + 1 \end{array}$$

Esta função associa a cada número inteiro x o número inteiro $f(x) = x + 1$. Em particular, temos que $f(0) = 1$, $f(-1) = 0$ e $f(1) = 2$.

2. A função $f: X \rightarrow X$, que ao elemento x associa o próprio x , recebe o nome de *função identidade* de X e é denotada por Id_X .

3. Seja $f: X \rightarrow Y$ uma função tal que existe $b \in Y$ com $f(x) = b$ para todo x de X . Este tipo de aplicação é chamado de *aplicação constante*.

4. Toda função $S: \mathbb{N} \rightarrow A$ é chamada de *seqüência* em A . Costuma-se escrever s_n no lugar de $s(n)$.

5. Sejam $f: X \rightarrow Y$ uma função e A um subconjunto de X . Podemos definir uma nova função $g: A \rightarrow Y$ com a mesma lei de f , isto é, $g(x) = f(x)$ para todo $x \in A$. Esta função é chamada de *restrição* de f a A e é denotada por $f|_A$ ou quando não houver risco de confusão, simplesmente por f .

6. Seja A um conjunto. Uma função qualquer $f: A \times A \rightarrow A$ é chamada de *operação* em A . Dizemos que a operação f é *comutativa* se $f(a, b) = f(b, a)$ para todo par (a, b) em $A \times A$.

A operação f é dita *associativa* se para todos os elementos a, b e c de A se tem

$$f(a, f(b, c)) = f(f(a, b), c).$$

Um elemento e de A é dito *elemento neutro* para a operação f se para todo elemento a de A se tem

$$f(a, e) = f(e, a) = a.$$

Se f possui um elemento neutro e , um elemento b de A é dito *elemento simétrico* de a se

$$f(a, b) = f(b, a) = e.$$

As funções

$$\begin{array}{ccc} + : \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (a, b) & \longmapsto & a + b \end{array} \quad , \quad \begin{array}{ccc} \cdot : \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

são exemplos de operações associativas comutativas e com elementos neutros respectivamente 0 e 1.

7. Sejam $X = \{a, b\}$ e $Y = \{1, 2\}$. Damos abaixo todas as funções de X em Y .

$$f_1: \begin{cases} a \mapsto 1 \\ b \mapsto 1 \end{cases} \quad f_2: \begin{cases} a \mapsto 2 \\ b \mapsto 2 \end{cases} \quad f_3: \begin{cases} a \mapsto 1 \\ b \mapsto 2 \end{cases} \quad f_4: \begin{cases} a \mapsto 2 \\ b \mapsto 1 \end{cases}$$

3.2. Composição de Funções

Dadas duas funções $f: X \rightarrow Y$ e $g: Y \rightarrow Z$, define-se uma nova função $h: X \rightarrow Z$ com a regra

$$h(x) = g(f(x)).$$

A função h é chamada de *função composta* de g com f e é denotada por $g \circ f$. Temos portanto, por definição, que

$$g \circ f(x) = g(f(x)).$$

Exemplos

1. Sejam

$$\begin{array}{rcl} f: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x + 1 \end{array}, \quad \begin{array}{rcl} g: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x^2 \end{array}$$

Considere as funções $f \circ g$ e $g \circ f$ de \mathbb{Z} em \mathbb{Z} . Temos que

$$f \circ g(x) = f(g(x)) = x^2 + 1,$$

enquanto que

$$g \circ f(x) = g(f(x)) = (x + 1)^2.$$

Este exemplo mostra que em geral se tem $f \circ g \neq g \circ f$.

2. Seja $f: X \rightarrow Y$ uma função. Temos que

$$f \circ \text{Id}_X(x) = f(\text{Id}_X(x)) = f(x),$$

e que

$$\text{Id}_Y \circ f(x) = \text{Id}_Y(f(x)) = f(x).$$

Logo, qualquer que seja a função $f: X \rightarrow Y$, tem-se que

$$f \circ \text{Id}_X = f \quad \text{e} \quad \text{Id}_Y \circ f = f.$$

3. Sejam

$$\begin{array}{rcl} f: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x + 1 \end{array}, \quad \begin{array}{rcl} g: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x - 1 \end{array}$$

Temos que $f \circ g = g \circ f = \text{Id}_{\mathbb{Z}}$.

4. Seja $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^3$. Considere a função $f^2 = f \circ f$. Temos que $f^2(x) = f \circ f(x) = (x^3)^3 = x^9$. Atenção, não confundir $f^2(x)$ com $(f(x))^2$, que neste caso é x^6 .

O processo de composição pode ser iterado. Dadas três funções, $f: X \rightarrow Y$, $g: Y \rightarrow Z$ e $h: Z \rightarrow W$, podemos compor estas funções de dois modos aparentemente distintos,

$$h \circ (g \circ f) \quad \text{e} \quad (h \circ g) \circ f.$$

Parece portanto ambíguo falar da composta $h \circ g \circ f$ das três funções mas, na verdade esta ambiguidade inexiste pois os dois modos de compor conduzem ao mesmo resultado como mostra a seguinte cadeia de igualdades

$$[h \circ (g \circ f)](x) = h(g \circ f(x)) = h(g(f(x))) = h \circ g(f(x)) = [(h \circ g) \circ f](x).$$

Está portanto bem definida a função $h \circ g \circ f: X \rightarrow W$.

3.3. Imagens Diretas e Inversas

Dada uma função $f: X \rightarrow Y$ e um subconjunto A de X , define-se a *imagem direta* de A por f como sendo

$$f(A) = \{y \in Y \mid y = f(x) \text{ para algum } x \text{ em } A\}.$$

Em particular, $f(X)$ é chamado simplesmente de *imagem* de f ou *codomínio* de f .

Se V é um subconjunto de Y , define-se a *imagem inversa* de V por f como sendo

$$f^{-1}(V) = \{x \in X \mid f(x) \in V\}.$$

Segue imediatamente das definições que $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$ e $f^{-1}(Y) = X$.

Problemas

3.1 Determine todas as funções de $X = \{a, b, c\}$ em $Y = \{1, 2\}$.

3.2 Sejam f , g e h funções de \mathbb{Z} em \mathbb{Z} tais que $h(1) = 3$, $g(3) = 2$ e $f(2) = 5$, calcule $f \circ g(3)$, $g \circ h(1)$ e $f \circ g \circ h(1)$.

3.3 Sejam

$$\begin{array}{rcl} f: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & ax + b \end{array}, \quad \begin{array}{rcl} g: \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & cx + d \end{array},$$

$$\begin{aligned} h: \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto kx^2 + \ell x + m \end{aligned}$$

onde a, b, c, d, k, ℓ e m são números inteiros. Determine as seguintes funções: $f \circ g$, $g \circ f$, $h \circ f$, $f \circ h$, g^2 , f^3 , h^2 e $g \circ h \circ f$.

3.4 Seja $f: X \rightarrow Y$ uma função. Se $A \subset B \subset X$ e $V \subset W \subset Y$, mostre que $f(A) \subset f(B)$ e $f^{-1}(V) \subset f^{-1}(W)$.

3.5 Seja $f: X \rightarrow Y$ uma função. Se $A, B \subset X$, mostre que

- a) $f(A \cup B) = f(A) \cup f(B)$.
- b) $f(A \cap B) \subset f(A) \cap f(B)$. Mostre com um exemplo que em geral não vale a igualdade.
- c) $f(A \setminus B) \supset f(A) \setminus f(B)$. Mostre com um exemplo que em geral não vale a igualdade.
- d) $f(f^{-1}(f(A))) = f(A)$.

3.6 Sejam $f: X \rightarrow Y$ uma função e $V, W \subset Y$. Mostre que

- a) $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$
- b) $f^{-1}(V \cap W) = f^{-1}(V) \cap f^{-1}(W)$
- c) $f^{-1}(V \setminus W) = f^{-1}(V) \setminus f^{-1}(W)$.

3.7 Sejam $f: X \rightarrow Y$ uma função e $A \subset X$, $V \subset Y$. Mostre que $A \subset f^{-1}(f(A))$ e $f(f^{-1}(V)) = V \cap f(X)$.

3.8 Sejam $f: X \rightarrow Y$, $g: Y \rightarrow Z$, $A \subset X$ e $V \subset Z$. Mostre que

- a) $(g \circ f)(A) = g(f(A))$
- b) $(g \circ f)^{-1}(V) = f^{-1}(g^{-1}(V))$.

4. Funções Bijetoras e Funções Inversas

4.1. Bijeções

Uma função $f: X \rightarrow Y$ será dita *injetora* se

$$\forall x_1, x_2 \in X, \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Isto equivale à seguinte implicação

$$\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2.$$

Uma função $f: X \rightarrow Y$ será dita *sobrejetora* se todo elemento de Y é imagem por f de algum elemento de X . Em outras palavras, f é sobrejetora se para todo $y \in Y$ existir $x \in X$ tal que $y = f(x)$; ou equivalentemente, se $f(X) = Y$.

Uma função é dita *bijetora* ou uma *bijeção* se ela é injetora e sobrejetora.

Exemplos

1. É bijetora a função

$$\begin{aligned} f: \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longrightarrow x + 1 \end{aligned}$$

2. A função

$$\begin{aligned} f: \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longrightarrow n^2 \end{aligned}$$

é injetora porém não sobrejetora.

3. Toda função $\text{Id}_X: X \rightarrow X$ é bijetora.

4. A função

$$\begin{aligned} f: \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longrightarrow 2 \end{aligned}$$

não é sobrejetora nem injetora.

4.2. Funções Inversas

Dada uma função $f: X \rightarrow Y$, dizemos que uma função $g: Y \rightarrow X$ é uma *inversa à esquerda* de f , se

$$g \circ f = \text{Id}_X.$$

Dizemos que g é uma inversa à direita de f , se

$$f \circ g = \text{Id}_Y.$$

Proposição 7. *Uma função é sobrejetora se e somente se ela admite inversa à direita.*

Demonstração: Seja $f: X \rightarrow Y$ uma função sobrejetora. Então para cada y em Y é possível escolher pelos menos um x em X tal que $y = f(x)$; fixe um tal x para cada y . Defina $g: Y \rightarrow X$ tal que $g(y) = x$ (note que em geral tal função g não é unicamente determinada, ela o será se f é injetora). Segue então, para todo $y \in Y$, que

$$f \circ g(y) = f(g(y)) = f(x) = y,$$

logo $f \circ g = \text{Id}_Y$ e portanto g é uma inversa à direita de f .

Reciprocamente, suponha que $f \circ g = \text{Id}_Y$ para alguma função $g: Y \rightarrow X$. Como Id_Y é sobrejetora, segue que f é também sobrejetora (Justifique. Veja Problema 4.3,b). \square

Proposição 8. *Uma função é injetora se e somente se ela admite uma inversa à esquerda.*

Demonstração: Seja $f: X \rightarrow Y$ uma função injetora. Então cada $y \in f(X)$ determina um único x em X tal que $y = f(x)$. Defina $g: Y \rightarrow X$ como segue:

$$g(y) = \begin{cases} x & , \text{ se } y = f(x) \\ \text{qualquer valor} & , \text{ se } y \notin f(X) \end{cases}$$

(Note que em geral g não é unicamente determinada, ela o será se f por sobrejetora). Segue então que

$$g \circ f(x) = g(f(x)) = g(y) = x,$$

para todo x em X , logo $g \circ f = \text{Id}_X$, e portanto g é uma inversa à esquerda de f .

Suponha reciprocamente que existe $g: Y \rightarrow X$ tal que $g \circ f = \text{Id}_X$. Como Id_X é injetora, segue que f é injetora (veja Problema 4.2 (b)). \square

Proposição 9. *Se uma função admite uma inversa à esquerda e uma inversa à direita, estas são iguais.*

Demonstração: Sejam $g_1, g_2: Y \rightarrow X$ respectivamente uma inversa à direita e uma inversa à esquerda de uma função $f: X \rightarrow Y$. Segue que

$$g_1 = \text{Id}_X \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \text{Id}_Y = g_2. \quad \square$$

Uma função $g: Y \rightarrow X$ é dita *função inversa* de $f: X \rightarrow Y$ se ela for simultaneamente função inversa à direita e à esquerda de f . Segue imediatamente da Proposição 9 que, se uma função admite função inversa, esta é única.

A proposição seguinte caracterizará as funções que admitem inversas

Proposição 10. *Uma função admite função inversa se e somente se ela é bijetora.*

Demonstração: Seja f uma função bijetora. Pelas Proposições 7 e 8, esta admite uma inversa à esquerda e uma inversa à direita, logo pela Proposição 9 estas são iguais, definindo uma função inversa para f . A reciproca também segue das Proposições 7 e 8. \square

Problemas

4.1 Para quais valores de a, b e c inteiros, a função $f: \mathbb{Z} \rightarrow \mathbb{Z}$, definida por $x \mapsto ax^2 + bx + c$ é bijetora?

4.2 Sejam $f: X \rightarrow Y$ e $g: Y \rightarrow Z$ funções. Demonstre que

- a) Se f e g são injetoras, então $g \circ f$ é injetora
- b) Se $g \circ f$ é injetora, então f é injetora
- c) Se $g \circ f$ é injetora e f é sobrejetora, então g é injetora

4.3 Sejam $f: X \rightarrow Y$ e $g: Y \rightarrow Z$ funções. Demonstre que

- a) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora
- b) Se $g \circ f$ é sobrejetora, então g é sobrejetora
- c) Se $g \circ f$ é sobrejetora e g é injetora, então f é sobrejetora

4.4 Sejam $f: X \rightarrow Y$ e $g: Y \rightarrow Z$ funções.

- a) Mostre que se f e g são bijetoras, então $g \circ f$ é bijetora
- b) Construa um exemplo que mostre que a recíproca de (a) é falsa
- c) Mostre que se f é bijetora então f^{-1} é bijetora

4.5 Seja $f: X \rightarrow Y$ uma função. Prove que f é sobrejetora se, e somente se, para todo conjunto Z e todo par de funções $g: Y \rightarrow Z$ e $h: Y \rightarrow Z$, $g \circ f = h \circ f$ implica $g = h$.

4.6 Seja $f: X \rightarrow Y$ uma função. Prove que f é injetora se, e somente se, para todo conjunto Z e todo par de funções $g: Z \rightarrow X$ e $h: Z \rightarrow X$, $f \circ g = f \circ h$ implica $g = h$.

4.7 Seja dada uma função $f: X \rightarrow Y$. Mostre que

- a) f é sobrejetora se, e somente se, para todo $B \subset Y$, $f(f^{-1}(B)) = B$
- b) f é injetora se, e somente se, para todo $A \subset X$, $f^{-1}(f(A)) = A$

4.8 Seja $f: X \rightarrow Y$ uma função. Mostre que f é injetora se, e somente se, para todo par de subconjuntos A e B de X , vale $f(A \setminus B) = f(A) \setminus f(B)$.

Os Números Inteiros e Racionais

Os números foram considerados durante milênios como entes intuitivos e algumas de suas propriedades, como por exemplo a comutatividade e a associatividade da adição e da multiplicação, eram consideradas inerentes à sua própria natureza, portanto não necessitando de demonstração.

O grande desenvolvimento da matemática a partir da criação do Cálculo Diferencial no século dezessete colocou diante dos matemáticos novos problemas que, para serem melhor compreendidos e solucionados, requeriam uma fundamentação mais rigorosa do conceito de número. Esta tarefa foi empreendida pelos matemáticos do século dezenove.

O primeiro a idealizar um método para a construção dos números inteiros negativos e dos números racionais a partir dos números naturais foi Karl Weierstrass. Bem mais sutil e profunda é a construção dos números irracionais, cuja descoberta de sua existência remonta à Grécia antiga, a partir dos números racionais, isto foi conseguido independentemente por Georg Cantor e Richard Dedekind por volta de 1870.

Os números naturais ainda resistiram às investidas por algum tempo. Segundo vários matemáticos da época não seria possível construir tais números. Ficou célebre a seguinte frase de Leopold Kronecker a tal propósito, “Deus criou os inteiros, todo o resto é obra do Homem”. O grande capítulo da construção dos números ficou encerrado quando em 1888 Dedekind publicou um trabalho onde, a partir de noções básicas da teoria dos conjuntos, ele constroi um modelo para

os números naturais, definindo as operações de adição e multiplicação e demonstrando as suas propriedades básicas. A construção de Dedekind não teve muita difusão na época por ser bastante complicada. Ficou entretanto mais popular a axiomática que Giuseppe Peano deu em 1889. Trata-se de um conjunto de quatro axiomas que caracterizam totalmente os naturais.

Não realizaremos toda a construção acima referida. Iniciaremos neste capítulo o estudo dos inteiros para os quais daremos um tratamento axiomático, tendo como ponto de partida uma lista de propriedades básicas que os caracterizarão completamente, para delas deduzir as demais propriedades. Em seguida construiremos o conjunto dos números racionais a partir dos inteiros. Esta construção será feita no contexto mais geral dos domínios de integridade pois não irá requerer nenhum esforço adicional e evitará que no futuro tenhamos que repetir esta mesma construção em outras situações análogas. Finalmente a construção dos números reais será realizada no Capítulo 8.

1. Os Números Inteiros

O conjunto \mathbb{Z} dos números inteiros é munido de duas operações, uma adição ($+$) e uma multiplicação (\cdot), além de uma relação de ordem (\leqslant). Estes objetos se relacionam através de várias propriedades que listaremos ao longo das três próximas sub-seções. Esta lista de propriedades caracterizará completamente os números inteiros de um modo que será precisado no Teorema 3 do Capítulo 3.

1.1. Anéis

Sejam A um conjunto e $(+)$ e (\cdot) duas operações em A , chamadas de adição e multiplicação. A terna $(A, +, \cdot)$ será chamada de *anél* se as operações gozarem das seguintes propriedades.

A₁ (A adição é associativa) *Quaisquer que sejam $a, b, c \in A$, tem-se que $(a + b) + c = a + (b + c)$.*

A₂ (A adição é comutativa) *Quaisquer que sejam $a, b \in A$ tem-se que $a + b = b + a$.*

A₃ (Existe um elemento neutro para a adição) *Existe $\alpha \in A$ tal que $\alpha + x = x$, para todo $x \in A$.*

A₄ (Todo elemento de A possui um simétrico) Para todo $a \in A$, existe $a' \in A$ tal que $a + a' = \alpha$.

M₁ (A multiplicação é associativa) Quaisquer que sejam $a, b, c \in A$, tem-se que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M₂ (A multiplicação é comutativa) Quaisquer que sejam $a, b \in A$, tem-se que $a \cdot b = b \cdot a$.

M₃ (Existe um elemento neutro para a multiplicação) Existe $e \in A$, com $e \neq 0$, tal que $x \cdot e = x$ para todo $x \in A$.

AM (A multiplicação é distributiva com relação à adição) Quaisquer que sejam $a, b, c \in A$, tem-se que

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Observações:

1. O elemento neutro da adição é único. De fato, sejam α e α' elementos neutros para a adição. Como α' é neutro, temos que

$$\alpha = \alpha' + \alpha,$$

e como α é neutro, temos que

$$\alpha' = \alpha + \alpha'.$$

Por A₂ temos então que $\alpha = \alpha'$.

Usaremos o símbolo 0 para denotar o elemento neutro da adição que será chamado de *zero*.

2. O elemento neutro da multiplicação é único. De fato, a demonstração acima devidamente adaptada nos fornece o resultado. Usaremos o símbolo 1 para denotar o elemento neutro da multiplicação que será chamado de *unidade*, ou apenas *um*.

3. O simétrico de um elemento $a \in A$ é único. De fato, se a' e a'' são dois simétricos de a , então por A₂ e A₁ temos que

$$a'' = 0 + a'' = (a' + a) + a'' = a' + (a + a'') = a' + 0 = a'.$$

Este (único) simétrico de a será simbolizado por $-a$. Note que o simétrico de $-a$ é a .

Usaremos a notação $a - b$ para representar $a + (-b)$. Esta operação em A é chamada de *subtração*.

Um elemento $a \in A$ será dito *invertível*, se existir um elemento $b \in A$ tal que $a \cdot b = 1$. Um tal elemento b será chamado de *inverso* de a . Note que o inverso de um elemento a , se existir, é único. De fato, se b e b' são inversos de a , temos que

$$b = b \cdot 1 = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = (a \cdot b) \cdot b' = 1 \cdot b' = b'.$$

No caso em que a é invertível, o seu (único) inverso será denotado por a^{-1} . Denotaremos por A^* o conjunto dos elementos invertíveis de um anel A . Note que se $x, y \in A^*$, então $x \cdot y \in A^*$ (veja Problema 1.3), isto é, A^* é fechado com respeito à multiplicação de A . Note também que $1 \in A^*$ e que se $x \in A^*$, então $x^{-1} \in A^*$ (pois segue da definição que o inverso de x^{-1} é o próprio x).

Um anel A será chamado de *domínio de integridade* ou simplesmente de *domínio* se for verificada a seguinte propriedade.

M₄ (Integridade) *Dados $a, b \in A$, se $a \neq 0$ e $b \neq 0$, então $a \cdot b \neq 0$.*

A propriedade acima é obviamente equivalente à seguinte propriedade:

M'₄. *Dados $a, b \in A$, se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

O seguinte axioma caracteriza parcialmente o conjunto dos inteiros e será complementado nas próximas duas sub-seções.

Axioma 1. $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade.

A seguir enunciamos e demonstramos algumas propriedades dos anéis que decorrem das definições. No que segue A designará um anel

Proposição 1. *Para todo $a \in A$, temos que $a \cdot 0 = 0$.*

Demonstração: Utilizando AM segue que

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Somando membro a membro $-(a \cdot 0)$ (que existe por A₄) na igualdade

$$a \cdot 0 = a \cdot 0 + a \cdot 0,$$

segue que

$$-(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0).$$

Por A₁ e A₂ temos que

$$0 = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0,$$

logo $a \cdot 0 = 0$. □

Num anel A o elemento zero nunca é invertível pois se fosse, existira $b \in A$ tal que $0 \cdot b = 1$, logo pela Proposição 1 teríamos $0 = 1$, o que é uma contradição pois por definição $1 \neq 0$.

Um anel A tal que todo elemento não nulo (i.e., diferente de zero) é invertível é chamado de *corpo*. Verifica-se facilmente que todo corpo é domínio de integridade (veja Problema 1.4).

Proposição 2. *Para todo $a \in A$, temos que $(-1) \cdot a = -a$.*

Demonstração: Por M₃, AM, A₄ e pela Proposição 1, temos que

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0.$$

Somando $-a$ a ambos os membros da igualdade $(-1) \cdot a + a = 0$ e usando A₁, A₄ e A₃, obtemos o resultado. □

Usando a Proposição 2, M₁ e M₃ é fácil mostrar que

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b).$$

Das igualdades acima segue a distributividade da multiplicação com relação à subtração, isto é, para todos $a, b, c \in A$, temos que

$$a \cdot (b - c) = a \cdot b - a \cdot c.$$

Proposição 3 (Lei do Cancelamento). *Seja A um domínio de integridade. Para todos $a, x, y \in A$ com $a \neq 0$, se $a \cdot x = a \cdot y$, então $x = y$.*

Demonstração: Somando $-(a \cdot x)$ a ambos os lados da igualdade $a \cdot x = a \cdot y$, e usando a observação após a Proposição 2 e AM, segue que

$$0 = a \cdot (y - x).$$

Como $a \neq 0$, por M'_4 segue que $y - x = 0$ e consequentemente $x = y$. \square

1.2. Anéis Ordenados

Uma *relação binária* num conjunto A é uma sentença aberta no conjunto $A \times A$.

Um anel A será chamado de *anel ordenado* se existir uma relação binária $x \leq y$, que se lê x é *menor do que ou igual* a y , que goza das seguintes propriedades:

O₁ (Reflexividade) *Para todo $a \in A$, temos que $a \leq a$.*

O₂ (Antisimetria) *Para todos $a, b \in A$, se $a \leq b$ e $b \leq a$, então $a = b$.*

O₃ (Transitividade) *Para todos $a, b, c \in A$, se $a \leq b$ e $b \leq c$, então $a \leq c$.*

O₄ (Totalidade) *Dados $a, b \in A$, tem-se que é verdadeira uma das asserções $a \leq b$ ou $b \leq a$.*

OA (Compatibilidade com a adição) *Para todos $a, b, c \in A$, se $a \leq b$, então $a + c \leq b + c$.*

OM (Compatibilidade com a multiplicação) *Para todos $a, b, c \in A$, se $a \leq b$ e $0 \leq c$, então $a \cdot c \leq b \cdot c$.*

Usaremos a notação $a < b$, que se lê a é *menor do que* b , para indicar que $a \leq b$ com $a \neq b$. Note que se $a < b$, então $a \leq b$. Usaremos também as notações $b > a$, que se lê b é *maior do que* a , e $b \geq a$, que se lê b é *maior do que ou igual* a a , significando $a < b$ e $a \leq b$, respectivamente.

Damos mais um passo na axiomatização do conjunto \mathbb{Z} dos inteiros, complementando o Axioma 1 como segue:

Axioma 2. $(\mathbb{Z}, +, \cdot, \leq)$ é um domínio ordenado.

Num anel ordenado define-se o *valor absoluto* de um elemento $a \in A$ como sendo,

$$|a| = \begin{cases} a & , \text{ se } a \geq 0 \\ -a & , \text{ se } a < 0 \end{cases}$$

Segue imediatamente desta definição que $|a| \geq 0$, para todo $a \in A$ e que vale a igualdade se e somente se $a = 0$.

Proposição 4. *Sejam A um anel ordenado e $a, b, r \in A$. Temos que*

- (i) $|a \cdot b| = |a| \cdot |b|$
- (ii) $-|a| \leq a \leq |a|$
- (iii) $|a| \leq r$ se e somente se $-r \leq a \leq r$
- (iv) $|a + b| \leq |a| + |b|$

Demonstração: i. Se $a \geq 0$ e $b \geq 0$, então de OM segue que $a \cdot b \geq 0$ e a igualdade segue imediatamente da definição. Se $a \geq 0$ e $b \leq 0$, então $a \cdot b \leq 0$ (veja Problema 1.8(c)) e neste caso temos da observação após a Proposição 2 que

$$|a \cdot b| = -(a \cdot b) = a \cdot (-b) = |a| \cdot |b|.$$

Os casos $a \leq 0$, $b \geq 0$ e $a \leq 0$, $b \leq 0$ são tratados de modo semelhante.

ii. Segue imediatamente da definição.

iii. Suponha que $|a| \leq r$. Segue então que $-|a| \geq -r$ (veja Problema 1.8(c)). Logo de (ii) temos que

$$-r \leq -|a| \leq a \leq |a| \leq r.$$

Reciprocamente, suponha que $-r \leq a \leq r$. Se $a \geq 0$, então $|a| = a \leq r$. Se $a < 0$, então $|a| = -a \leq r$ (a última desigualdade pode ser obtida somando a ambos os membros de $-r \leq a$ o elemento $r - a$).

iv. Somando membro a membro as desigualdades

$$-|a| \leq a \leq |a| \quad \text{e} \quad -|b| \leq b \leq |b|,$$

obtemos (veja Problemas 1.1(c) e 1.6(b))

$$-(|a| + |b|) \leq a + b \leq |a| + |b|,$$

logo de (iii) segue que $|a + b| \leq |a| + |b|$. □

Corolário 1. *Sejam A um anel ordenado e $a, b \in A$. Temos que*

$$||a| - |b|| \leq |a \pm b| \leq |a| + |b|.$$

Demonstração: A desigualdade $|a + b| \leq |a| + |b|$ foi provada na proposição. Novamente pela proposição temos,

$$|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|.$$

Agora, pela proposição temos

$$|a| = |a + b - a| \leq |a + b| + |-a| = |a + b| + |a|,$$

logo

$$|a| - |b| \leq |a + b|.$$

Por outro lado,

$$|b| = |b + a - a| \leq |b + a| + |-a| = |a + b| + |a|,$$

logo,

$$-|a + b| \leq |a| - |b|.$$

Portanto

$$-|a + b| \leq |a| - |b| \leq |a + b|,$$

e consequentemente pelo ítem (iii) da proposição temos que

$$||a| - |b|| \leq |a + b|.$$

A desigualdade $|a - b| \geq ||a| - |b||$ segue imediatamente da desigualdade acima. \square

1.3. Anéis Bem Ordenados

Um subconjunto S de um anel ordenado A será dito *limitado inferiormente* (respectivamente, *superiormente*), se existir um elemento $a \in A$ tal que para todo $x \in S$ se tenha $x \geq a$ (respectivamente, $x \leq a$). O conjunto vazio é considerado limitado inferiormente e superiormente.

Diremos que S tem um *menor elemento* (respectivamente, *maior elemento*), se existir $b \in S$ tal que para todo $x \in S$ se tenha $x \geq b$ (respectivamente, $x \leq b$). Se existir um menor elemento de um subconjunto S de um anel ordenado A , este é único. De fato, se b e b' são menores elementos de S , temos que $b \leq b'$ e $b' \leq b$, logo pela antisimetria da relação de ordem \leq , segue que $b = b'$. No caso em que existe o menor elemento de S , ele é denotado por $\min S$. A mesma observação vale para o maior elemento que será denotado por $\max S$.

Um domínio ordenado A será chamado de *domínio bem ordenado* se gozar da seguinte propriedade.

PBO (Princípio da Boa Ordenação) *Todo subconjunto não vazio de A limitado inferiormente possui um menor elemento.*

A propriedade acima é equivalente à seguinte propriedade.

PBO'. *Todo subconjunto não vazio de A limitado superiormente possui um maior elemento.*

De fato, isto segue das seguintes observações fáceis de verificar. Seja $\emptyset \neq S \subset A$, defina $S' = \{-b \mid b \in S\}$. Então S é limitado inferiormente se e somente se S' é limitado superiormente. Tem-se também que S possui um menor elemento se e somente se S' possui um maior elemento (neste caso tem-se que $\min S = -\max S'$).

Daremos a seguir a axiomática completa para os números inteiros.

Axiomas dos números inteiros. $(\mathbb{Z}, +, \cdot, \leq)$ é um domínio bem ordenado.

Demonstraremos no Capítulo 3 que existe essencialmente um único domínio bem ordenado (num sentido que precisaremos na próxima sub-seção).

A seguir damos alguns resultados característicos dos domínios bem ordenados.

Proposição 5. *Sejam A um domínio bem ordenado e $a \in A$. Se $a > 0$, então $a \geq 1$.*

Demonstração: Suponha por absurdo que exista $a \in A$ tal que $0 < a < 1$, logo o conjunto

$$S = \{x \in A \mid 0 < x < 1\}$$

é não vazio e limitado inferiormente. Portanto S possui um menor elemento b tal que $0 < b < 1$. Segue então que $0 < b^2 < b < 1$ e consequentemente $b^2 \in S$ e $b^2 < b$, absurdo. \square

Corolário 1. *Sejam A um domínio bem ordenado e $a, b \in A$. Se $a > b$, então $a \geq b + 1$.*

Demonstração: Aplique a proposição com $a - b$ no lugar de a . \square

Corolário 2. Sejam A um domínio bem ordenado e $a, b \in A$ com $b \neq 0$. Então $|a \cdot b| \geq |a|$.

Demonstração: Como $b \neq 0$, pela Proposição 5 temos que $|b| \geq 1$. Multiplicando ambos os membros desta igualdade por $|a|$, segue da Proposição 4 (i) que

$$|a \cdot b| = |a| \cdot |b| \geq |a|. \quad \square$$

Proposição 6. Seja A um domínio bem ordenado e $a, b \in A$. Se $a \cdot b = 1$, então $a = b = 1$, ou $a = b = -1$.

Demonstração: Se $a \cdot b = 1$, segue da Proposição 1 que $a \neq 0$ e $b \neq 0$. Logo pelo Corolário 2 acima e o fato de $1 > 0$ (veja Problema 1.9(b)), temos que $1 = |a \cdot b| \geq |a|$ e $1 = |a \cdot b| \geq |b|$. Como $|a| > 0$ e $|b| > 0$, segue pela Proposição 5 que $|a| = |b| = 1$ e portanto $a = \pm 1$ e $b = \pm 1$. Da hipótese $a \cdot b = 1$ segue que $a = b = 1$ ou $a = b = -1$. \square

A proposição acima mostra que os únicos elementos invertíveis de um domínio bem ordenado são 1 e -1 .

Proposição 7 (Propriedade Arquimediana). Dados elementos a e b de um domínio bem ordenado A com $b \neq 0$, existe um elemento $n \in A$ tal que $n \cdot b \geq a$.

Demonstração: Como $b \neq 0$, temos pela Proposição 4 (i) e pelo Corolário 2 da Proposição 5, que

$$|b| \cdot |a| = |b \cdot a| \geq |a| \geq a.$$

Se $b > 0$, tome $n = |a|$ e o resultado segue da desigualdade acima. Se $b < 0$, tome $n = -|a|$ é o resultado também segue da desigualdade acima. \square

1.4. Homomorfismos

As funções naturais no âmbito dos anéis são aquelas que preservam as operações. Tais funções serão chamadas de homomorfismos. Precisamente, dados dois anéis A e B , uma função $f: A \rightarrow B$ será chamada

de *homomorfismo* se valerem para todos os elementos a e b de A as igualdades:

- 1) $f(a + b) = f(a) + f(b)$
- 2) $f(a \cdot b) = f(a) \cdot f(b)$
- 3) $f(1) = 1.$

Note que as operações efetuadas nos primeiros membros das igualdades acima são em A enquanto que as dos segundos membros são em B .

Um homomorfismo bijetor será chamado de *isomorfismo*. É fácil verificar que a função inversa de um isomorfismo é um homomorfismo (veja Proposição 8). Dois anéis que admitem entre si um isomorfismo são ditos *isomorfos* e no que diz respeito à estrutura de anel eles são considerados iguais. Quando existir um isomorfismo entre dois anéis A e B escrevemos $A \simeq B$.

Se A e B são anéis ordenados e $f: A \rightarrow B$ é um homomorfismo tal que se $a \leq b$, então $f(a) \leq f(b)$, diremos que f é um *homomorfismo de anéis ordenados*. Se o homomorfismo de anéis ordenados $f: A \rightarrow B$ for um isomorfismo, diremos que A e B são *isomorfos como anéis ordenados*. Provaremos no Capítulo 3 (Teorema 3) que dois domínios bem ordenados quaisquer são sempre isomorfos como anéis ordenados.

Um subconjunto A' de um anel A será chamado de *subanel* de A se A' , juntamente com as restrições a ele das operações de adição e de multiplicação de A , é um anel cujo elemento unidade é o elemento unidade de A .

Para provar que um subconjunto A' de A é um subanel de A é preciso verificar que 0 e 1 são elementos de A' , que a soma e o produto de dois elementos quaisquer de A' estão em A' e que o simétrico de todo elemento de A' está em A' . As demais propriedades de um anel são automaticamente satisfeitas para os elementos de A' pois o são para todos os elementos de A .

Proposição 8. *Seja $f: A \rightarrow B$ um homomorfismo de anéis. Temos que*

- (i) $f(0) = 0$
- (ii) *Quaisquer que sejam $a, b \in A$, temos que $f(a - b) = f(a) - f(b)$.*

Em particular, $f(-a) = -f(a)$

- (iii) *$f(A)$ é um subanel de B*
- (iv) *Se f é bijetora, então $f^{-1}: B \rightarrow A$ é um homomorfismo de anéis.*

Demonstração: i. Note que

$$f(0) = f(0 + 0) = f(0) + f(0),$$

logo, somando $-f(0)$ a ambos os lados da igualdade acima, temos que $f(0) = 0$

ii. Observe inicialmente que

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a),$$

logo $f(-a) = -f(a)$. Agora,

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b).$$

iii. de (i) temos que $0 \in f(A)$ e da definição, $1 = f(1) \in f(A)$. Que somas e produtos de elementos de $f(A)$ estão em $f(A)$ segue das condições (1) e (2) da definição de homomorfismo. Que o simétrico de um elemento de $f(A)$ está em $f(A)$ segue de (ii).

iv. Suponha f bijetora e sejam $y, y' \in B$. Logo existem $x, x' \in A$ univocamente determinados tais que $f(x) = y$ e $f(x') = y'$. Temos então que $f^{-1}(y + y') = f^{-1}(f(x) + f(x')) = f^{-1}(f(x + x')) = x + x' = f^{-1}(y) + f^{-1}(y')$, e também que $f^{-1}(y \cdot y') = f^{-1}(f(x) \cdot f(x')) = f^{-1}(f(x \cdot x')) = x \cdot x' = f^{-1}(y) \cdot f^{-1}(y')$. Finalmente é claro que $f^{-1}(1) = 1$. \square

Proposição 9. *Sejam $f: A \rightarrow B$ e $g: B \rightarrow C$ homomorfismos de anéis. Então $g \circ f: A \rightarrow C$ é um homomorfismo de anéis. Se f e g são isomorfismos, então $g \circ f$ é um isomorfismo.*

Demonstração: A prova deste resultado não contém nenhuma dificuldade e a deixamos como exercício. \square

Problemas

1.1 Mostre que num anel valem as seguintes propriedades

- a) Se $a + c = b + c$, então $a = b$;
- b) Se $a + b = a$ para algum a então $b = 0$;
- c) $-(a + b) = -a - b$;
- d) -1 é invertível.

1.2 Mostre que num domínio de integridade valem as seguintes propriedades

- a) $a^2 = 0$ se e somente se $a = 0$
- b) $a \cdot b = a$ se e somente se $a = 0$ ou $b = 1$
- c) $a^2 = a$ se e somente se $a = 0$ ou $a = 1$

1.3 Mostre que a e b são invertíveis se e somente se $a \cdot b$ é invertível. Mostre que neste caso se tem $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

1.4 Mostre que todo corpo é domínio de integridade.

1.5 Sejam A um anel e $a \in A \setminus \{0\}$. Defina a função $f_a: A \rightarrow A$ pela lei $f_a(x) = a \cdot x$

- a) Mostre que f_a é sobrejetora se e somente se a é invertível
- b) Mostre que se A é um domínio, então f_a é injetora.

1.6 Mostre que num anel ordenado valem as seguintes propriedades

- a) Se $a + c \leq b + c$, então $a \leq b$
- b) Se $a \leq b$ e $c \leq d$, então $a + c \leq b + d$
- c) Se $a \leq b$ e $c \leq 0$, então $a \cdot c \geq b \cdot c$.

1.7 Mostre que num anel ordenado vale o seguinte:

- a) Se $a < b$ e $b < c$, então $a < c$;
- b) Se $a < b$ e $b \leq c$, então $a < c$;
- c) Se $a < b$, então $a + c < b + c$ para todo c .

1.8 Mostre que num anel ordenado vale o seguinte:

- a) Se $a \geq 0$, então $-a \leq 0$;

- b) Se $a \leq 0$, então $-a \geq 0$;
- c) Se $a \geq 0$ e $b \leq 0$, então $a \cdot b \leq 0$;
- d) Se $a \leq 0$ e $b \leq 0$, então $a \cdot b \geq 0$.

1.9 Mostre que num anel ordenado vale o seguinte:

- a) Para todo a , tem-se que $a^2 \geq 0$;
- b) $1 > 0$;
- c) $-1 < 0$.

1.10 Mostre que num domínio ordenado se $a < b$ e $c > 0$, então $a \cdot c < b \cdot c$.

1.11 Mostre que num domínio ordenado vale o seguinte:

- a) Se $a \cdot c \leq b \cdot c$ e $c > 0$, então $a \leq b$
- b) Se $a \cdot c \leq b \cdot c$ e $c < 0$, então $a \geq b$

1.12 Seja $f: A \rightarrow B$ um homomorfismo de anéis. Mostre que se $a \in A$ é invertível, então $f(a)$ é invertível e $(f(a))^{-1} = f(a^{-1})$.

2. Os Números Racionais

O que é um número racional? Usualmente define-se um número racional como sendo uma fração $\frac{a}{b}$ com a e b números inteiros e $b \neq 0$. Mas o que é uma fração? O essencial numa fração $\frac{a}{b}$ é o par ordenado (a, b) e a relação de igualdade:

$$\frac{a}{b} = \frac{a'}{b'} \iff a \cdot b' = a' \cdot b.$$

Isto é o ponto de partida para definir o corpo de frações de um domínio de integridade qualquer. Em particular, quando o domínio é \mathbb{Z} obtemos o corpo dos números racionais.

2.1. Corpo de Frações de um Domínio de Integridade

Seja A um domínio de integridade. Considere o seguinte conjunto,

$$B = \{(a, b) \in A \times A \mid b \neq 0\}.$$

Defina em B a seguinte relação binária:

$$(a, b) \sim (a', b') \Leftrightarrow a \cdot b' = a' \cdot b.$$

Esta relação possui as seguintes propriedades:

Reflexividade: $(a, b) \sim (a, b)$ para todo $(a, b) \in B$

Simetria: Se $(a, b) \sim (a', b')$, então $(a', b') \sim (a, b)$

Transitividade: Se $(a, b) \sim (a', b')$ e $(a', b') \sim (a'', b'')$, então $(a, b) \sim (a'', b'')$.

As duas primeiras propriedades seguem imediatamente da definição e a terceira propriedade se demonstra como segue:

Se $(a, b) \sim (a', b')$ e $(a', b') \sim (a'', b'')$, então $a \cdot b' = a' \cdot b$ e $a' \cdot b'' = a'' \cdot b'$. Multiplicando a primeira igualdade por b'' e a segunda por b segue que

$$a \cdot b' \cdot b'' = a' \cdot b \cdot b'' = a'' \cdot b' \cdot b,$$

logo

$$(a \cdot b'' - a'' \cdot b) \cdot b' = 0.$$

Como A é um domínio de integridade e $b' \neq 0$, segue que

$$a \cdot b'' - a'' \cdot b = 0$$

e consequentemente $(a, b) \sim (a'', b'')$.

Uma relação binária que possui as três propriedades acima é chamada de *relação de equivalência*. Tais relações aparecem frequentemente em matemática. Por exemplo, a igualdade é uma relação de equivalência. No Capítulo 6 veremos outros exemplos de relações de equivalência.

A *classe de equivalência* de um elemento (a, b) de B é o conjunto

$$\frac{a}{b} = \{(x, y) \in B \mid (x, y) \sim (a, b)\},$$

e o par (a, b) é chamado de *representante* da classe $\frac{a}{b}$.

Seja K o conjunto de todas as classes de equivalência de elementos de B :

$$K = \left\{ \frac{a}{b} \mid a, b \in A \text{ com } b \neq 0 \right\}$$

É fácil verificar que $\frac{a}{b} = \frac{c}{d}$ se somente se $(a, b) \sim (c, d)$ e portanto, se e somente se $a \cdot d = b \cdot c$.

Definimos em K as seguintes operações:

$$\text{Adição: } \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}.$$

$$\text{Multiplicação: } \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Antes de mais nada, é preciso verificar que estas leis efetivamente definem duas operações. Para isto é necessário mostrarmos que os resultados além de pertencerem a K , independem dos particulares representantes de $\frac{a}{b}$ e $\frac{c}{d}$. De fato, sendo A um domínio de integridade e como $b \neq 0$ e $d \neq 0$, segue que $b \cdot d \neq 0$, logo os resultados da adição e da multiplicação pertencem a K . Por outro lado, se $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$, não é difícil verificar (faça-o) que valem as igualdades

$$\frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{a' \cdot d' + b' \cdot c'}{b' \cdot d'},$$

e

$$\frac{a \cdot c}{b \cdot d} = \frac{a' \cdot c'}{b' \cdot d'},$$

logo os resultados independem dos particulares representantes de $\frac{a}{b}$ e $\frac{c}{d}$.

Teorema 1. *Com as operações acima definidas K é um corpo.*

Demonstração: Levando em conta que o elemento zero em K é $\frac{0}{1}$, que o simétrico de $\frac{a}{b}$ é $-\frac{a}{b}$ e que a unidade é $\frac{1}{1}$, a demonstração de que K é um anel é só uma série de verificações diretas que deixamos a cargo do leitor. Para provar que K é um corpo, seja $\frac{a}{b}$ um elemento não nulo de K . Sendo $b \neq 0$ e sendo a não nulo por ser $\frac{a}{b}$ não nulo, temos que $\frac{b}{a} \in K$ e

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1}{1}.$$

Portanto $\frac{a}{b}$ é invertível e $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. □

O corpo K é chamado de *corpo de frações* de A . O corpo de frações de \mathbb{Z} é o *corpo dos números racionais* \mathbb{Q} .

Considere a função

$$\begin{aligned} j: A &\longrightarrow K \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

Esta função é um homomorfismo injetor de anéis (verifique). Portanto temos um isomorfismo de A com o subanel $j(A)$ de K . Identificaremos o elemento a de A com $j(a) = \frac{a}{1} \in K$ que passa a ser denotado simplesmente por a .

Proposição 10. *Seja A um domínio com corpo de frações K . Se K' é um corpo e $f: A \rightarrow K'$ é um homomorfismo injetor de anéis, então existe um único homomorfismo de anéis $\tilde{f}: K \rightarrow K'$ tal que $\tilde{f} \circ j = f$.*

Demonstração: Se existisse \tilde{f} tal que $\tilde{f} \circ j = f$, teríamos para $\frac{a}{b} \in K$,

$$\begin{aligned} \tilde{f}\left(\frac{a}{b}\right) &= \tilde{f}\left(\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}\right) \\ &= \tilde{f}\left(\frac{a}{1}\right) \cdot \tilde{f}\left(\left(\frac{b}{1}\right)^{-1}\right) \\ &= \tilde{f}\left(\frac{a}{1}\right) \left(\tilde{f}\left(\frac{b}{1}\right)\right)^{-1} = f(a) \cdot (f(b))^{-1}, \end{aligned}$$

onde a igualdade $\tilde{f}\left(\left(\frac{b}{1}\right)^{-1}\right) = (\tilde{f}\left(\frac{b}{1}\right))^{-1}$ decorre do Problema 1.12.

Isto toma conta da unicidade de \tilde{f} . Agora basta mostrar que a aplicação

$$\begin{aligned} \tilde{f}: K &\longrightarrow K' \\ \frac{a}{b} &\longmapsto f(a)(f(b))^{-1} \end{aligned}$$

é um homomorfismo de anéis.

\tilde{f} é bem definida pois, como f é injetora tem-se que se $b \neq 0$, então $f(b) \neq 0$ e portanto $f(a)(f(b))^{-1}$ está bem definido como elemento de K' . Por outro lado, se $\frac{a}{b} = \frac{a'}{b'}$, então $a'b = b'a$ e portanto,

$$f(a')f(b) = f(a'b) = f(b'a) = f(b')f(a)$$

e consequentemente

$$f(a')(f(b'))^{-1} = f(a)(f(b))^{-1}.$$

Temos ainda que

$$\begin{aligned}
 \tilde{f}\left(\frac{a}{b} + \frac{a'}{b'}\right) &= \tilde{f}\left(\frac{ab' + a'b}{bb'}\right) = f(ab' + a'b)(f(bb'))^{-1} \\
 &= [f(a)f(b') + f(a')f(b)](f(b))^{-1}(f(b'))^{-1} \\
 &= f(a)(f(b))^{-1} + f(a')(f(b'))^{-1} \\
 &= \tilde{f}\left(\frac{a}{b}\right) + \tilde{f}\left(\frac{a'}{b'}\right)
 \end{aligned}$$

e que

$$\begin{aligned}
 \tilde{f}\left(\frac{a}{b} \cdot \frac{a'}{b'}\right) &= \tilde{f}\left(\frac{a \cdot a'}{b \cdot b'}\right) = f(a \cdot a')(f(b \cdot b'))^{-1} \\
 &= f(a)(f(b))^{-1} \cdot f(a')(f(b'))^{-1} \\
 &= \tilde{f}\left(\frac{a}{b}\right) \cdot \tilde{f}\left(\frac{a'}{b'}\right).
 \end{aligned}$$

Como $\tilde{f}\left(\frac{1}{1}\right) = f(1)(f(1))^{-1} = 1$, segue que \tilde{f} é um homomorfismo de anéis. \square

2.2. Corpo de Frações de um Domínio Ordenado

Sejam a e b elementos de um domínio ordenado A e seja K o corpo de frações de A . Devido à igualdade $\frac{a}{b} = \frac{-a}{-b}$ (verifique), todo elemento de K pode ser posto sob a forma $\frac{a}{b}$ com $b > 0$. Nesta seção vamos supor que todos os elementos de K estão sob esta forma.

Sejam dados $\frac{a}{b}$ e $\frac{c}{d}$ em K com $b > 0$ e $d > 0$. Definimos

$$\frac{a}{b} \leqslant \frac{c}{d} \iff a \cdot d \leqslant b \cdot c.$$

Suponha que $a \leqslant b$, logo $\frac{a}{1} \leqslant \frac{b}{1}$ e portanto $j(a) \leqslant j(b)$. Isto significa que a relação \leqslant em K acima definida estende a relação \leqslant de A .

Teorema 2. *Se A é um domínio ordenado, então o seu corpo de frações K é um anel ordenado.*

Demonstração: A relação de ordem de K é a relação \leqslant que definimos acima. Deixamos a cargo do leitor a verificação da reflexividade e da

antisimetria de \leqslant , enquanto que a transitividade se demonstra como segue:

Suponha que $\frac{a}{b} \leqslant \frac{c}{d}$ e $\frac{c}{d} \leqslant \frac{e}{f}$. Segue que $a \cdot d \leqslant b \cdot c$ e $c \cdot f \leqslant d \cdot e$. Multiplicando ambos os lados da primeira desigualdade por f e da segunda por b (lembre que $b > 0$ e $f > 0$), obtemos que $a \cdot d \cdot f \leqslant b \cdot c \cdot f$ e $b \cdot c \cdot f \leqslant b \cdot d \cdot e$. Pela transitividade da relação \leqslant em A , temos que $a \cdot d \cdot f \leqslant b \cdot d \cdot e$. Como $d > 0$, segue que $a \cdot f \leqslant b \cdot e$ (veja Problema 1.11 (a)), logo $\frac{a}{b} \leqslant \frac{e}{f}$.

Para provar a totalidade, considere a, b, c e d elementos de A com $b > 0$ e $d > 0$. Pela totalidade da relação \leqslant em A segue que $a \cdot d \leqslant b \cdot c$ ou $b \cdot c \leqslant a \cdot d$, logo uma das seguintes possibilidades é verificada:

$$\frac{a}{b} \leqslant \frac{c}{d} \quad \text{ou} \quad \frac{c}{d} \leqslant \frac{a}{b}.$$

A seguir demonstraremos a compatibilidade da relação \leqslant com a adição, deixando a verificação da propriedade análoga para a multiplicação a cargo do leitor.

Sejam $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d} \in K$ tais que $\frac{a}{b} \leqslant \frac{a'}{b'}$. Segue que $a \cdot b' \leqslant a' \cdot b$. Multiplicando ambos os lados desta última desigualdade por d^2 e somando $c \cdot d \cdot b' \cdot b$ a ambos os lados da desigualdade obtida, temos por OM e OA que

$$b' \cdot d \cdot (a \cdot d + b \cdot c) \leqslant b \cdot d \cdot (a' \cdot d + b' \cdot c),$$

onde segue que $\frac{a}{b} + \frac{c}{d} \leqslant \frac{a'}{b'} + \frac{c}{d}$. □

Um corpo que é ordenado como anel será chamado de *corpo ordenado*.

O corpo dos números racionais é uma extensão do anel dos números inteiros. O que ganhamos e o que perdemos com esta extensão? Inicialmente ganhamos o fato de termos preservado a estrutura de anel ordenado de \mathbb{Z} obtendo além disso a propriedade adicional de corpo, isto é, todo elemento não nulo de \mathbb{Q} passa a ser invertível em \mathbb{Q} . Esta propriedade é mais forte do que a de integridade (veja o Problema 1.4). Perde-se porém a propriedade característica de \mathbb{Z} que é o Princípio da Boa Ordenação como se pode verificar no seguinte exemplo. O conjunto $S = \{x \in \mathbb{Q} \mid 0 < x < 1\}$ é não vazio e limitado

inferiormente porém não possui menor elemento.

Problemas

2.1 Demonstre o Teorema 1.

2.2 Seja K' o corpo de frações de um corpo K . Considere a aplicação

$$\begin{aligned}\varphi: K' &\longrightarrow K \\ \frac{a}{b} &\longmapsto a \cdot b^{-1}\end{aligned}$$

Mostre que φ é um isomorfismo.

2.3 Faça as verificações deixadas a cargo do leitor na demonstração do Teorema 2.

2.4 Sejam a, b, c e d elementos de um corpo K com $b, d \neq 0$. Mostre que se $\frac{a}{b} = \frac{c}{d}$, então

- a) $\frac{a+c}{b+d} = \frac{a}{b}$, se $b+d \neq 0$;
- b) $\frac{a+b}{b} = \frac{c+d}{d}$;
- c) $\frac{a}{c} = \frac{b}{d}$, se $c \neq 0$;
- d) $\frac{a-b}{b} = \frac{c-d}{d}$;
- e) $\frac{a+b}{a-b} = \frac{c+d}{c-d}$, se $a \neq b$ e $c \neq d$.

2.5 Sejam $a, b \in \mathbb{Q}$. Mostre que $a > b > 0$ se e somente se $0 < \frac{1}{a} < \frac{1}{b}$.

2.6 Prove a seguinte propriedade de \mathbb{Q} (Propriedade Arquimediana): Dados $a, b \in \mathbb{Q}$ com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $n \cdot b \geq a$.

2.7 Sejam A um domínio ordenado, K' um corpo ordenado e $f: A \rightarrow K'$ um homomorfismo injetor de anéis ordenados. Mostre que o homomorfismo \tilde{f} da Proposição 10 é um homomorfismo de anéis ordenados onde a ordenação de K' é a do Teorema 2.

Propriedades dos Inteiros

1. Indução Matemática

A indução matemática é um poderoso instrumento para demonstrar teoremas que envolvem os inteiros e vem sendo utilizada de uma forma implícita desde a antiguidade. Foi explicitamente enunciada pela primeira vez por Francesco Maurolycus em 1575 e por ele usada, por exemplo, para provar a fórmula do problema 1.1(a). O método tornou-se popular após a publicação em 1665 do “Traité du triangle arithmétique” por Blaise Pascal onde era utilizado.

1.1. Princípio de Indução Matemática

Teorema 1 (Princípio de Indução Matemática). Seja $P(n)$ uma sentença aberta em $\{n \in \mathbb{Z} \mid n \geq n_0\}$, onde $n_0 \in \mathbb{Z}$, tal que,

- (i) $P(n_0)$ é verdadeira;
- (ii) Para todo $n \geq n_0$, se $P(n)$ é verdadeira, então $P(n + 1)$ é verdadeira.

Então $P(n)$ é verdadeira para todo $n \geq n_0$.

Demonstração: Seja $F = \{n \in \mathbb{Z} \mid n \geq n_0 \text{ e } P(n) \text{ é falsa}\}$. É claro que F é limitado inferiormente. Queremos provar que F é vazio. Suponha por absurdo que $F \neq \emptyset$, logo pelo Princípio da Boa Ordenação temos que F possui um menor elemento b . Como $b \in F$ temos que $b \geq n_0$, mas por (i) temos que $n_0 \notin F$, logo $b \neq n_0$ e portanto $b > n_0$. Segue pelo Corolário 1 da Proposição 5, Capítulo 2, que $b - 1 \geq n_0$. Sendo b o menor elemento de F , temos que $b - 1 \notin F$, logo $P(b - 1)$ é verdadeira.

De (ii) segue então que $P(b)$ é verdadeira, portanto $b \notin F$, contradição.

□

Chamamos a atenção do leitor para não confundir indução matemática com indução empírica. Nas ciências naturais é comum após um certo número (sempre finito) de experimentos, enunciar leis gerais que governam o fenômeno em estudo. Tais leis são tidas como verdadeiras até prova em contrário. A indução matemática serve para estabelecer verdades matemáticas, válidas em conjuntos infinitos. Não se trata de mostrar que uma certa sentença aberta é verdadeira para um grande número de inteiros mas, trata-se de provar que uma tal sentença é verdadeira para todo inteiro n com $n \geq n_0$.

A título de exemplo, considere a sentença aberta em \mathbb{N} :

$$P(n): \quad n = n + (n - 1) \cdot (n - 2) \cdots (n - 1000).$$

É claro que $P(1), P(2), P(3), \dots, P(1000)$ são verdadeiras. O leitor mais afoito poderia considerar que estes experimentos são suficientes para concluir que $P(n)$ é verdadeira para todo número natural n . Isto porém não é indução matemática. A conclusão seria falsa pois $P(1001)$ é falsa.

Exemplo: Vamos provar que a seguinte sentença aberta $P(n)$ é verdadeira para todo n natural.

$$P(n): \quad 1 + \cdots + n = \frac{n(n+1)}{2}.$$

(i) $P(1)$ é verdadeira pois $1 = 1(1+1)/2$.

(ii) Supondo $P(n)$ verdadeira temos que

$$1 + \cdots + n = \frac{(n+1)}{2},$$

somando $n+1$ a ambos os membros da igualdade, obtemos

$$1 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

logo $P(n+1)$ é verdadeira. Pelo Princípio de Indução Matemática $P(n)$ é verdadeira para todo $n \geq 1$.

A seguir daremos várias aplicações do Princípio de Indução Matemática.

1.2. Conjuntos Finitos e Infinitos

Seja $m \in \mathbb{N}$, definimos I_m como sendo o conjunto

$$I_m = \{x \in \mathbb{N} \mid x \leq m\} = \{1, \dots, m\}.$$

Diremos que um conjunto A é *finito*, se $A = \emptyset$ ou se existirem $m \in \mathbb{N}$ e uma bijeção de I_m em A . Se A não é finito, diremos que é *infinito*.

A questão que nos colocamos agora é saber se o número natural m é univocamente determinado por A e pela existência de uma bijeção de I_m em A . A resposta é positiva e decorre do seguinte resultado.

Teorema 2. *Sejam m e n dois números naturais. Se $m > n$, então não existe nenhuma função injetora de I_m em I_n .*

Demonstração: Basta provar o teorema quando $m = n + 1$. De fato, se $m > n + 1$ e se existisse uma função injetora de I_m em I_n , a sua restrição a I_{n+1} seria também injetora.

Mostraremos por indução sobre n que é verdadeira para todo $n \geq 1$ a seguinte asserção:

$P(n)$: Não existe nenhuma função injetora de I_{n+1} em I_n .

- (i) É claro que $P(1)$ é verdadeira;
- (ii) Suponhamos que $P(n)$ é verdadeira e seja $f: I_{n+2} \rightarrow I_{n+1}$, queremos provar que f não é injetora. Suponha por absurdo que f é injetora. Duas possibilidades podem ocorrer.
 - a) $n + 1 \notin f(I_{n+2})$. Neste caso, a função $g: I_{n+1} \rightarrow I_n$, definida por $g(x) = f(x)$ para todo $x \in I_{n+1}$ é injetora, o que é uma contradição.
 - b) $n + 1 \in f(I_{n+2})$. Seja x' o único elemento de I_{n+2} tal que $f(x') = n + 1$. Consideraremos dois subcasos:
 - b') $x' = n + 2$. Neste caso, $g: I_{n+1} \rightarrow I_n$ definida por $g(x) = f(x)$, $\forall x \in I_{n+1}$ é bem definida e injetora, absurdo.
 - b'') $x' \neq n + 2$. Como f é injetora, temos que $f(n+2) \neq f(x') = n + 1$.

Logo a função $g: I_{n+1} \rightarrow I_n$ definida por

$$g(x) = \begin{cases} f(x) & \text{se } x \neq x' \\ f(n+2) & \text{se } x = x' \end{cases}$$

é bem definida e injetora, contradição. \square

Suponha agora que dado um conjunto A , existam números naturais m e n com $m > n$ e duas bijeções $f: I_m \rightarrow A$ e $g: I_n \rightarrow A$. Segue então que $g^{-1} \circ f: I_m \rightarrow I_n$ é uma bijeção, portanto injetora o que não é possível pelo teorema. Consequentemente dado um conjunto finito A o número natural m para o qual existe uma bijeção $I_m \rightarrow A$ é univocamente determinado por A e é chamado do *número de elementos* de A . Diremos neste caso que A tem m elementos.

Corolário 1 (Princípio de Dirichlet). *Dados dois conjuntos X e Y respectivamente com m e n elementos, se $m > n$, então não existe nenhuma função injetora de X em Y .*

Demonstração: Existem bijeções $f: I_m \rightarrow X$ e $g: I_n \rightarrow Y$. Se existisse uma função injetora $h: X \rightarrow Y$, teríamos que $g^{-1} \circ h \circ f: I_m \rightarrow I_n$ é injetora, o que não é possível pelo teorema. \square

O Princípio de Dirichlet é também chamado de *princípio das gavetas* pois admite a seguinte formulação:

Dados m objetos a serem distribuídos em n gavetas e se $m > n$, então uma das gavetas deverá conter mais de um objeto.

Corolário 2. *Sejam X um conjunto com m elementos e Y um conjunto com n elementos. Se $m < n$, então não existe nenhuma sobrejeção de X em Y .*

Demonstração: Suponha que exista uma sobrejeção f de X em Y , logo pela Proposição 7 do Capítulo 1, f admite uma inversa à direita $g: Y \rightarrow X$. Portanto, $f \circ g = \text{Id}_Y$. Segue então que g admite uma inversa à esquerda. Pela Proposição 8 do Capítulo 1, tem-se que g é injetora. Isto contradiz o Princípio de Dirichlet. \square

Corolário 3. *Sejam X e Y dois conjuntos finitos com o mesmo número de elementos. Uma função $f: X \rightarrow Y$ é injetora se, e somente se, ela é sobrejetora.*

Demonstração: Suponha que f seja injetora e suponha por absurdo que não seja sobrejetora. Seja $y' \in Y$ não pertencente a $f(X)$. Logo é bem definida e injetora a função:

$$\begin{aligned} f_1: X &\longrightarrow Y \setminus \{y'\} \\ x &\longmapsto f(x) \end{aligned}$$

Isto é uma contradição pelo Princípio de Dirichlet.

Suponha agora que f seja sobrejetora mas não injetora. Logo existem x' e x'' em X tais que $f(x') = f(x'')$. Portanto é bem definida e sobrejetora a função:

$$\begin{aligned} f_2: X \setminus \{x'\} &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned}$$

Isto contradiz o Corolário 2. □

Corolário 4. *Todo domínio de integridade finito é um corpo.*

Demonstração: Seja A um tal domínio. Para $a \neq 0$, considere a função

$$\begin{aligned} f: A &\longrightarrow A \\ x &\longmapsto a \cdot x \end{aligned}$$

Esta função é injetora (veja Problema 1.5, Capítulo 2). Logo pelo Corolário 3, esta função é sobrejetora. Portanto, existe um elemento b em A tal que $a \cdot b = f(b) = 1$. Com isto fica provado que todo elemento $a \neq 0$ possui um inverso. Portanto, A é um corpo. □

Para $n \in \mathbb{Z}^+$, define-se o *fatorial* de n como sendo

$$n! = \begin{cases} 1 & , \text{ se } n = 0 \text{ ou } n = 1 \\ 1 \cdot 2 \cdots n & , \text{ se } n > 1 \end{cases}$$

Proposição 1. *Dados dois conjuntos A e B com n elementos, então o conjunto de todas as bijeções de A tem $n!$ elementos.*

Demonstração: Considere a sentença aberta

$P(n)$: O número de bijeções entre dois conjuntos, cada um contendo n elementos, é $n!$.

$P(1)$ é claramente verdadeira pois só existe uma bijeção entre dois conjuntos com 1 elemento cada um.

Suponha $P(n)$ verdadeira e sejam A e B dois conjuntos com $n+1$ elementos cada um. Fixe um elemento a de A . Existem $n+1$ possibilidades para escolher a imagem de a em B por uma bijeção. Para cada escolha destas, por exemplo $a \mapsto b$, as bijeções que têm esta propriedade são tantas quantas são as bijeções de $A \setminus \{a\}$ em $B \setminus \{b\}$, logo são em número $n!$. Portanto o número total de possibilidades de definir uma bijeção de A em B é

$$(n+1) \cdot n! = (n+1)!.$$

□

Daremos agora um exemplo de conjunto infinito

Proposição 2. \mathbb{Z} é infinito.

Demonstração: Se existissem um número natural m e uma bijeção $f: I_m \rightarrow \mathbb{Z}$, teríamos uma função injetora $f^{-1}: \mathbb{Z} \rightarrow I_m$ e portanto a restrição $f^{-1}|_{I_{m+1}}: I_{m+1} \rightarrow I_m$ seria injetora, o que é impossível pelo Teorema 2. □

1.3. O Homomorfismo Característico

Sejam dados um anel A , um elemento a de A e um inteiro n . Definimos

$$na = \begin{cases} 0 & , \text{ se } n = 0 \\ a + (n-1)a & , \text{ se } n \geq 1 \\ -((-n)a) & , \text{ se } n < 0 \end{cases}$$

Proposição 3. Para todo $a \in A$ e todos $m, n \in \mathbb{Z}$, temos

- (i) $m(a + b) = ma + mb$
- (ii) $m(a \cdot b) = (ma) \cdot b$
- (iii) $(m + n)a = ma + na$
- (iv) $(m \cdot n)a = m(na)$
- (v) $(-m)a = -(ma)$

Demonstração: A demonstração destes fatos é deixada a cargo do leitor, veja Problema 1.9. \square

Das propriedades acima segue imediatamente que a aplicação natural

$$\begin{aligned}\rho: \mathbb{Z} &\longrightarrow A \\ n &\longmapsto n1\end{aligned}$$

é um homomorfismo de anéis, chamado de *homomorfismo característico*. O próximo resultado nos garantirá que este é o único homomorfismo de \mathbb{Z} em A .

Proposição 4. Se $h: \mathbb{Z} \rightarrow A$ é um homomorfismo de anéis, então $h = \rho$.

Demonstração: Note que pela Proposição 8 (i) do Capítulo 2, temos que $h(0) = \rho(0) = 0$. Vamos provar por indução sobre n que para todo $n > 0$, temos que

$$h(n) = n1. \quad (1)$$

Para $n = 1$, isto é claro pois $h(1) = 1$. Suponha que para algum valor de $n > 0$, a igualdade (1) é verificada, logo

$$h(n+1) = h(n) + h(1) = n1 + 1 = (n+1)1,$$

o que demonstra, pelo Princípio de Indução Matemática, a igualdade (1) para todo $n > 0$.

Por outro lado, pela Proposição 8(ii), Capítulo 2 e pelo caso $n > 0$ que acabamos de provar, temos que se $n < 0$, então

$$h(n) = -h(-n) = -(-n)1 = n1.$$

Com isto acabamos de provar que

$$h(n) = n1 = \rho(n) , \quad \forall n \in \mathbb{Z}. \quad \square$$

Corolário. Seja K um corpo tal que o homomorfismo característico $\rho: \mathbb{Z} \rightarrow K$ é injetor. Então existe um único homomorfismo $\tilde{\rho}: \mathbb{Q} \rightarrow K$ e este é tal que $\tilde{\rho} \circ j = \rho$, onde $j: \mathbb{Z} \rightarrow \mathbb{Q}$ é o homomorfismo característico.

Demonstração: A existência de $\tilde{\rho}$ é garantida pela Proposição 10 do Capítulo 2. Para provar a unicidade, suponha que tenhamos um homomorfismo

$$h: \mathbb{Q} \rightarrow K$$

Logo temos dois homomorfismos ρ e $h \circ j$ de \mathbb{Z} em K e portanto pela Proposição 4, segue que $h \circ j = \rho$. Novamente, a Proposição 10 do Capítulo 2 nos diz que $h = \tilde{\rho}$. \square

O homomorfismo característico ρ desempenha papel importante na teoria dos anéis. Para anéis ordenados, ρ tem a seguinte propriedade adicional.

Proposição 5. *Se A é um anel ordenado, então ρ é um homomorfismo injetor de anéis ordenados.*

Demonstração: Inicialmente provaremos por indução que se $n \in \mathbb{N}$, então $n1 > 0$.

Para $n = 1$, isto é claro já que em qualquer anel ordenado temos $1 > 0$ (veja Problema 1.9 (b), Capítulo 2). Suponha agora que para um determinado $n > 0$ tenhamos $n1 > 0$. Somando o elemento 1 de A a ambos os membros da última desigualdade acima, temos

$$(n + 1)1 = n1 + 1 > 1 > 0,$$

Obtendo $(n + 1)1 > 0$. Consequentemente, para todo $n > 0$, temos que $n1 > 0$. Disto segue que se $n < 0$, então $n1 < 0$.

Suponha que $m < n$, logo $n - m > 0$ e portanto $(n - m)1 > 0$, obtendo

$$\rho(n) - \rho(m) = n1 - m1 = (n - m)1 > 0,$$

logo $\rho(m) < \rho(n)$. Isto mostra que ρ é um homomorfismo injetor de anéis ordenados. \square

Corolário. *Seja K um corpo ordenado. Existe um único homomorfismo $\tilde{\rho}: \mathbb{Q} \rightarrow K$. Além disso, $\tilde{\rho}$ é um homomorfismo de anéis ordenados.*

Demonstração: Isto segue imediatamente da Proposição 5 e do Corolário da Proposição 4. Resta apenas provar que $\tilde{\rho}$ é um homomorfismo de anéis ordenados, o que segue do Problema 2.7, Capítulo 2.

\square

Teorema 3. *Se A é um domínio bem ordenado, então ρ é um isomorfismo de anéis ordenados.*

Demonstração: Da Proposição 5 temos que ρ é um homomorfismo injetor de anéis ordenados. Falta apenas provar que ρ é sobrejetor, o que equivale a mostrar que todo elemento $a \in A$ é da forma $n1$ para algum $n \in \mathbb{Z}$. Suponha por absurdo que existe $a \in A$ tal que $n1 \neq a$ para todo $n \in \mathbb{Z}$. Considere os subconjuntos de A

$$S_1 = \{n1 \mid n \in \mathbb{Z} \text{ e } n1 > a\}$$

e

$$S_2 = \{n1 \mid n \in \mathbb{Z} \text{ e } n1 < a\}.$$

Mostraremos que $S_1 = S_2 = \emptyset$, o que é uma contradição.

Suponha que $S_1 \neq \emptyset$. Sendo S_1 limitado inferiormente, pelo Princípio da Boa Ordenação, ele possui um menor elemento $m1$, logo $m1 > a$ e $(m-1)1 \leq a$. Como $(m-1)1 \neq a$, temos que $(m-1)1 < a$ e consequentemente pelo Corolário da Proposição 5, Capítulo 2, temos que

$$m1 = (m-1)1 + 1 \leq a,$$

contradição.

De modo análogo prova-se que $S_2 = \emptyset$, usando porém a formulação (PBO') do Princípio da Boa Ordenação. \square

O teorema acima nos garante que a menos de isomorfismo, \mathbb{Z} é o único anel bem ordenado.

1.4. Binômio de Newton

Sejam A um anel, $a \in A$ e $n \in \mathbb{N}$. Definimos

$$a^n = \begin{cases} a & , \text{ se } n = 1 \\ a \cdot a^{n-1} & , \text{ se } n > 1 \end{cases}$$

Se $a \neq 0$, definimos $a^0 = 1$ e se a é invertível e $n < 0$, definimos $a^n = (a^{-1})^{-n}$.

Usando a definição acima é possível verificar (veja Problema 1.10) que para todos $a, b \in A \setminus \{0\}$ e todos $m, n \in \mathbb{Z}^+$, temos que

- (i) $a^m \cdot a^n = a^{m+n}$;
- (ii) $(a^m)^n = a^{m \cdot n}$;

$$(iii) \quad a^n \cdot b^n = (a \cdot b)^n.$$

E se a é invertível, as igualdades acima se estendem para $n, m \in \mathbb{Z}$.

Para $n, i \in \mathbb{Z}^+$, definimos

$$\binom{n}{i} = \begin{cases} \frac{n!}{i!(n-i)!} & , \text{ se } n \geq i \\ 0 & , \text{ se } n < i \end{cases}$$

Pela definição destes números não é claro que se trata de números inteiros. Os próximos lemas nos mostrarão que tais números são efectivamente inteiros.

Lema 1 (Relação de Stifel). *Para todo número natural n e todo inteiro i com $1 \leq i \leq n$, tem-se que*

$$\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$$

Demonstração:

$$\begin{aligned} \binom{n}{i-1} + \binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} \\ &= \frac{i \cdot n! + (n-i+1) \cdot n!}{i!(n-i+1)!} \\ &= \frac{(n+1) \cdot n!}{i!(n-i+1)!} = \frac{(n+1)!}{i!(n-i+1)!} = \binom{n+1}{i} \end{aligned}$$

□

Lema 2. *Dado um número natural n qualquer, para todo número inteiro i com $0 \leq i \leq n$, é inteiro o número $\binom{n}{i}$.*

Demonstração: Por indução sobre n . A proposição é claramente verdadeira para $n = 1$. Suponha que seja verdadeira para n .

$\binom{n+1}{0} = \binom{n+1}{n+1} = 1$, logo inteiros. Se $1 \leq i \leq n$, temos pelo lema 1 que

$$\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i}$$

logo inteiro pela hipótese de indução. □

Teorema 4 (Binômio de Newton). *Dados dois elementos a e b de um anel e um número natural n , tem-se que*

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} \cdot b + \cdots + \binom{n}{i} a^{n-i} \cdot b^i + \cdots + b^n$$

Demonstração: Seja $P(n)$ a igualdade acima. $P(1)$ é obviamente verdadeira. Suponhamos que $P(n)$ seja verdadeira. Temos que

$$(a + b)^{n+1} = (a + b) \cdot (a + b)^n = a \cdot (a + b)^n + b \cdot (a + b)^n$$

Pela hipótese de que $P(n)$ é verdadeira, segue que

$$\begin{aligned} a \cdot (a + b)^n &= a^{n+1} + \binom{n}{1} a^n \cdot b + \binom{n}{2} a^{n-1} \cdot b^2 + \\ &\quad + \cdots + \binom{n}{n-1} a^2 \cdot b^{n-1} + \binom{n}{n} a \cdot b^n \\ b \cdot (a + b)^n &= a^n b + \binom{n}{1} a^{n-1} \cdot b^2 + \\ &\quad + \cdots + \binom{n}{n-2} a^2 \cdot b^{n-1} + \binom{n}{n-1} a \cdot b^n + b^{n+1} \end{aligned}$$

Somando membro a membro estas igualdades e usando as relações do Lema 1, segue que $P(n + 1)$ é verdadeira. \square

Corolário. *Para todo número natural n , tem-se que*

$$\begin{aligned} (a - b)^n &= a^n + \binom{n}{1} (-1) a^{n-1} \cdot b + \cdots + \\ &\quad \binom{n}{i} (-1)^i a^{n-i} \cdot b^i + \cdots + (-1)^n b^n. \end{aligned}$$

Exemplos: Aplicando a fórmula do binômio de Newton segue que

$$(a + b)^2 = a^2 + 2a \cdot b + b^2$$

$$(a + b)^3 = a^3 + 3a^2 \cdot b + 3a \cdot b^2 + b^3$$

$$(a + b)^4 = a^4 + 4a^3 \cdot b + 6a^2 \cdot b^2 + 4a \cdot b^3 + b^4$$

1.5. Desigualdade de Bernoulli

Teorema 5 (Desigualdade de Bernoulli). *Seja A um domínio ordenado e seja $c \in A$ tal que $c \geq -1$, então para todo número natural n vale a seguinte desigualdade:*

$$(1 + c)^n \geq 1 + nc.$$

Demonstração: Seja $P(n)$ a desigualdade acima.

- (i) $P(1)$ é claramente verdadeira
- (ii) Suponha $P(n)$ verdadeira. Multiplicando ambos os lados da desigualdade acima por $1 + c$ (que é ≥ 0), obtemos

$$(1 + c)^{n+1} \geq (1 + n \cdot c)(1 + c) = 1(n + 1)c + nc^2 \geq 1 + (n + 1)c,$$

onde concluímos que $P(n + 1)$ é verdadeira.

Pelo Princípio de Indução Matemática segue que $P(n)$ é verdadeira para todo número natural n . \square

Corolário. *Dados $b, c \in \mathbb{Q}$ com $b > 1$, existe $n \in \mathbb{N}$ tal que $b^n > c$.*

Demonstração: Se $c \leq 0$, a desigualdade acima é claramente satisfeita para todo n . Suponha que $c > 0$. De $b > 1$ segue que $b - 1 \neq 0$, logo pela propriedade arquimediana de \mathbb{Q} (veja Problema 2.6, Capítulo 2) existe $n \in \mathbb{Z}$ tal que $n(b - 1) \geq c$. Como $c > 0$ e $b - 1 > 0$ segue que $n \in \mathbb{N}$. Temos então pela desigualdade de Bernoulli que

$$b^n = (1 + (b - 1))^n \geq 1 + n(b - 1) > n(b - 1) \geq c. \quad \square$$

O corolário acima nos afirma que as potências de expoente inteiro positivo de um número racional maior do que 1 formam um conjunto que não é limitado superiormente.

Problemas

1.1 Prove por indução as seguintes fórmulas:

- (a) $1 + 3 + 5 + \cdots + (2n - 1) = n^2$;
- (b) $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$;

- (c) $1^3 + 2^3 + 3^3 + \cdots + n^3 = [n(n+1)/2]^2$;
- (d) $1^4 + 2^4 + 3^4 + \cdots + n^4 = n(n+1)(2n+1)(3n^2+3n-1)/30$.

1.2 Prove por indução que:

- a) $n! \geq 2^n$ para todo $n \geq 4$;
- b) $n! \geq 3^n$ para todo $n \geq 7$;
- c) $n! \geq 4^n$ para todo $n \geq 9$.

1.3 Ache o erro na “demonstração” da seguinte afirmação obviamente falsa: Todos os números inteiros positivos são iguais, ou seja, para todo $n \in \mathbb{N}$ é verdadeira a asserção $P(n)$: $1 = \cdots = n$

- (i) $P(1)$ é verdadeira pois $1 = 1$;
- (ii) Suponha $P(n)$ verdadeira, logo $1 = \cdots = n - 1 = n$. Somando 1 a cada membro da última igualdade, segue que $n = n + 1$, logo $1 = \cdots = n - 1 = n = n + 1$ e portanto $P(n + 1)$ é verdadeira.

Pelo Princípio da Indução Matemática segue que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

1.4 Dada a sentença aberta $P(n)$: $1 + 2 + \cdots + n = [n(n+1)/2] + 1$, em \mathbb{N} , mostre que

- (i) Para todo $n \in \mathbb{N}$, se $P(n)$ é verdadeira então $P(n + 1)$ é verdadeira;
- (ii) $P(n)$ não é verdadeira para nenhum n .

1.5 Seja $f: \mathbb{Z} \rightarrow \mathbb{Z}$ uma função tal que quaisquer que sejam a e b , $f(a + b) = f(a) + f(b)$

- a) Mostre que $f(0) = 0$;
- b) Mostre por indução que $f(n) = n \cdot f(1)$ para todo $n \in \mathbb{Z}^+$;
- c) Mostre que $f(-n) = -f(n)$ para todo $n \in \mathbb{Z}$;
- d) Conclua que $f(n) = n \cdot f(1)$ para todo $n \in \mathbb{Z}$.

1.6 Uma *Progressão Aritmética* (P.A.) com primeiro termo a_1 e razão r é uma seqüência de números cujo primeiro elemento é a_1 e tal que

cada elemento, a partir do segundo, é igual ao anterior mais a razão. Em símbolos, se $n \geq 2$, $a_n = a_{n-1} + r$

- Prove por indução sobre n que $a_n = a_1 + (n - 1)r$;
- Se $S_n = a_1 + a_2 + \cdots + a_n$, prove por indução sobre n que

$$S_n = \frac{n(a_1 + a_n)}{2}.$$

1.7 Uma *Progressão Geométrica* (P.G.) com primeiro termo a_1 e razão q ($q \neq 0$ e $q \neq 1$) é uma seqüência de números cujo primeiro elemento é a_1 e tal que, cada elemento, a partir do segundo, é igual ao anterior multiplicado pela razão. Em símbolos, se $n \geq 2$, $a_n = a_{n-1} \cdot q$

- Prove por indução sobre n que $a_n = a_1 \cdot q^{n-1}$;
- Se $S_n = a_1 + a_2 + \cdots + a_n$, prove por indução sobre n que

$$S_n = \frac{a_n \cdot q - a_1}{q - 1}.$$

1.8 Este é um jogo antigo chamado Torre de Hanoi. Dispõe-se de n discos perfurados de diâmetros decrescentes enfiados numa haste A, e de duas outras hastas B e C.

O problema consiste em transferir toda a pilha de discos para a haste C, deslocando um disco de cada vez para qualquer haste, de modo que nenhum disco seja colocado sobre um outro de diâmetro menor

- Se a_n é o menor número de jogadas que resolve o jogo com n discos, mostre que $a_1 = 1$ e se $n \geq 2$, então $a_n = 2a_{n-1} + 1$;
- Mostre, por indução sobre n , que se $n \geq 1$, então $a_n = 2^n - 1$.

1.9 Sejam A um anel, a e b elementos de A e n e m inteiros. Verifique que:

- | | |
|---------------------------|---------------------------|
| a) $(m \cdot n)a = m(na)$ | b) $m(a \cdot b) = (ma)b$ |
| c) $(m + n)a = ma + na$ | d) $m(a + b) = ma + mb$ |
| e) $(-m)a = -(ma)$ | |

1.10 Sejam A um anel, a e b elementos de $A \setminus \{0\}$ e m e n números naturais. Mostre que

- a) $a^n \cdot a^m = a^{n+m}$;
- b) $(a^n)^m = a^{n \cdot m}$;
- c) $a^n \cdot b^n = (a \cdot b)^n$.

Mostre que se a é invertível, então as igualdades acima se estendem para $n, m \in \mathbb{Z}$.

1.11 Fazendo $a = b = 1$ no Teorema do Binômio de Newton e no seu Corolário verifique que

- a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$
- b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$

2. Divisão com Resto

A divisão nos inteiros nem sempre é exata. Poder efetuar a divisão de dois inteiros com resto pequeno é uma propriedade importante responsável por propriedades algébricas notáveis que os inteiros possuem.

Teorema 6 (Divisão Euclidiana). *Dados inteiros d e D com $d \neq 0$, existem inteiros q e r tais que*

$$D = d \cdot q + r \quad e \quad 0 \leq r < |d|.$$

Além disso, q e r são unicamente determinados pelas condições acima.

Demonstração: Considere o conjunto limitado inferiormente,

$$S = \{x \in \mathbb{Z}^+ \mid x = D - d \cdot n \text{ para algum } n \in \mathbb{Z}\}.$$

Este conjunto é não vazio pois pela Propriedade Arquimediana dos inteiros, Proposição 7, Capítulo 2, existe um inteiro n tal que $n \cdot (-d) \geq -D$, portanto $x = D - n \cdot d \in S$.

Pelo Princípio da Boa Ordenação, segue que S possui um menor elemento r . Logo $r = D - d \cdot q$, para algum $q \in \mathbb{Z}$. É claro que $r \geq 0$ pois $r \in S$. Vamos agora provar que $r < |d|$.

Suponha por absurdo que $r \geq |d|$, logo $r = |d| + s$ para algum inteiro s tal que $0 \leq s < r$. Portanto

$$D = d \cdot q + |d| + s = d(q \pm 1) + s,$$

e consequentemente,

$$s = D - d \cdot (q \pm 1) \in S.$$

Como $s \in S$ e $s < r$, temos uma contradição pois r era o menor elemento de S .

Para provar a unicidade, suponha que

$$D = d \cdot q_1 + r_1 = d \cdot q_2 + r_2,$$

com $0 \leq r_1 < |d|$ e $0 \leq r_2 < |d|$. Por estas últimas desigualdades segue que

$$-|d| < -r_2 \leq r_1 - r_2 \quad \text{e} \quad r_1 - r_2 < |d| - r_2 \leq |d|,$$

e portanto

$$-|d| < r_1 - r_2 < |d|.$$

Consequentemente, pela Proposição 4 (iii), Capítulo 2, temos que $|r_1 - r_2| < |d|$. Como

$$d(q_1 - q_2) = r_2 - r_1,$$

segue da Proposição 4 (i), Capítulo 2, que

$$|d| \cdot |q_1 - q_2| = |r_2 - r_1| < |d|.$$

Isto só é possível se $q_1 = q_2$ e $r_2 = r_1$. □

O teorema nos garante portanto que em \mathbb{Z} é possível efetuar a divisão de um número D por outro número $d \neq 0$ com resto pequeno. Os números D , d , q e r são chamados respectivamente de *dividendo*, *divisor*, *quociente* e *resto*.

A função *parte inteira* desempenha papel importante em Teoria dos Números e é definida como segue

$$\begin{aligned} [\quad]: \mathbb{Q} &\longrightarrow \mathbb{Z} \\ x &\longmapsto [x] = \text{maior inteiro } \leq x \end{aligned}$$

Por exemplo, $[1/2] = 0$, $[-1/2] = -1$, $[3/2] = 1$.

Observações

1. Na divisão euclidiana, se $D \geq 0$ e $d > 0$, então $q \geq 0$. De fato, se valesse $q < 0$, teríamos

$$D = d \cdot q + r < d \cdot q + d = d(q + 1) \leq 0,$$

logo $D < 0$, absurdo.

2. Na divisão euclidiana, se $D \geq d > 0$, então $r < D/2$. De fato, como $D = d \cdot q + r$ com $0 \leq r < d$. É claro que $q \neq 0$ pois caso contrário, teríamos $D = r < d$, contrário à hipótese de que $D \geq d$. Logo pela Observação 1 temos que $q > 0$ e consequentemente $q \geq 1$. Disto e da desigualdade $r < d$, obtemos $r \leq r_q < dq$, portanto, $D = d \cdot q + r > 2r$, consequentemente, $r < D/2$.

3. O Teorema 6 admite a seguinte generalização: Dados inteiros D , d , n e m com $d \neq 0$ e $n \neq 0$, existem inteiros q e r unicamente determinados pelas condições

$$D = d \cdot q + r \quad \text{e} \quad \frac{m}{n} \leq r < \frac{m}{n} + |d|.$$

O Teorema 6 corresponde ao caso $\frac{m}{n} = 0$. Quando $\frac{m}{n} = -\frac{|d|}{2}$, esta divisão se chama de *algoritmo do menor resto*. Neste caso, tem-se que

$$-\frac{|d|}{2} \leq r < \frac{|d|}{2}.$$

4. Sejam $a, b \in \mathbb{Z}$ com $b > 0$ e q o quociente da divisão de a por b . Então $q = [\frac{a}{b}]$.

De fato, sendo $a = b \cdot q + r$ com $0 \leq r < b$, segue que $\frac{a}{b} = q + \frac{r}{b}$ com $\frac{r}{b}$ um número racional tal que $0 \leq \frac{r}{b} < 1$. Portanto,

$$q \leq \frac{a}{b} = q + \frac{r}{b} < q + 1,$$

logo $q = [\frac{a}{b}]$.

5. Dado um número racional c , existe um número inteiro no intervalo

$$(c, c + 1] = \{x \in \mathbb{Q} \mid c < x \leq c + 1\}.$$

De fato, suponha $c = \frac{a}{b}$ com $a, b \in \mathbb{Z}$ e $b > 0$. Pela Observação acima,

$$[c] = \frac{a}{b} - \frac{r}{b},$$

com $0 \leq \frac{r}{b} < 1$ e portanto,

$$0 < ([c] + 1) - c \leq 1,$$

logo $[c] + 1 \in (c, c + 1]$.

Note que existe um único inteiro no intervalo $(c, c + 1]$. Vale um resultado análogo para o intervalo $[c, c + 1)$.

Problemas

2.1 Ache q e r na divisão euclidiana quando:

- | | | |
|----------------------|----------------------|---------------------|
| a) $D = 25, d = 7$ | b) $D = -25, d = 7$ | c) $D = 25, d = -7$ |
| d) $D = -25, d = -7$ | e) $D = 8, d = 10$ | f) $D = -8, d = 10$ |
| g) $D = 8, d = -10$ | h) $D = -8, d = -10$ | |

2.2 Se o quociente e o resto da divisão de a por b são respectivamente q e r , quais são o quociente e o resto da divisão de a por $-b$? E de $-a$ por b ?

2.3 Quais são os números inteiros que quando divididos por 4 dão um resto igual

- | | |
|----------------------------|-----------------------------|
| a) à metade do quociente ? | b) ao quociente ? |
| c) ao dobro do quociente ? | d) ao triplo do quociente ? |

2.4 A soma dos quocientes na divisão euclidiana de dois números D e D' por um número $d > 0$, é sempre igual ao quociente da divisão de $D + D'$ por d ? Se não for igual de quanto difere?

2.5 Usando a divisão euclidiana, mostre que todo número inteiro é da forma $2n$ ou $2n + 1$ com $n \in \mathbb{Z}$. Os números da forma $2n$ são chamados *pares* e os da forma $2n + 1$ são chamados *ímpares*. Mostre que:

- a) a soma de dois números pares é par;
- b) a soma de dois números ímpares é par;

- c) a soma de um número par com um ímpar é ímpar;
- d) o produto de dois números é par se um deles é par;
- e) o produto de dois números ímpares é ímpar;
- f) de dois inteiros consecutivos um deles é par.

2.6 Seja a um número inteiro qualquer. Mostre que exatamente um número de cada terna dada é divisível por 3

- | | |
|-----------------------|------------------------|
| a) $a, a + 1, a + 2$ | b) $a, a + 2, a + 4$ |
| c) $a, a + 5, a + 10$ | d) $a, a + 10, a + 20$ |

2.7 Seja a um número inteiro. Mostre que

- a) se a^2 é par, então a é par;
- b) se a^2 é divisível por 3, então a é divisível por 3.

2.8 Sejam $m, n, a \in \mathbb{N}$ com $n > m > 1$

- a) Quantos inteiros divisíveis por a existem entre 1 e n ?
- b) Quantos existem entre m e n ?
- c) Quantos inteiros divisíveis por 7 existem entre 112 e 1328?

3. Sistemas de Numeração

Nesta seção vamos nos ocupar com a representação dos números inteiros. Há vários modos de se representar números inteiros e a cada um desses chamamos de *sistema de numeração*. A maioria dos sistemas de numeração tem em comum o fato dos números serem representados pelo uso de um número reduzido de símbolos chamados *algarismos*. Os sistemas de numeração mais utilizados são os sistemas de base constante e se baseiam no seguinte resultado.

Teorema 7. *Dados inteiros a e b com $a \geq 0$ e $b > 1$, existem inteiros $c_0, c_1, \dots, c_n, \dots$, univocamente determinados pelas seguintes condições:*

- (i) *Existe um número natural m tal que $c_n = 0$ para todo $n \geq m$;*
- (ii) *Para todo n , temos que $0 \leq c_n < b$;*

$$(iii) \quad a = c_0 + c_1 \cdot b + \cdots + c_n \cdot b^n + \cdots$$

Demonstração: Fixe um inteiro $b > 1$. Seja S o conjunto dos elementos de \mathbb{Z}^+ para os quais são satisfeitas as condições do teorema. Queremos provar que o complementar S' de S em \mathbb{Z}^+ é vazio. Caso $S' \neq \emptyset$, como é limitado inferiormente, ele possui um menor elemento c . Pela Divisão Euclidiana, temos que

$$c = b \cdot q + r \quad , \quad 0 \leq r < b.$$

Como $c, b > 0$, temos que $q \geq 0$ (veja Observação 1 após o Teorema 6) e claramente $q < c$, logo $q \in S$. Portanto

$$q = c_1 + c_2 \cdot b + \cdots + c_n \cdot b^{n-1}$$

com c_i únicos tais que $0 \leq c_i < b$ para todo $i = 1, \dots, n$.

Se tomarmos $c_0 = r$, temos que

$$c = c_0 + c_1 \cdot b + \cdots + c_n \cdot b^n$$

com c_i tais que $0 \leq c_i < b$ para todo $i = 0, \dots, n$.

Suponha agora que $c = c'_0 + q' \cdot b$, com $0 \leq c'_0 < b$ e

$$q' = c'_1 + c'_2 \cdot b + \cdots + c'_m b^{m-1}.$$

Pela unicidade do quociente e do resto na divisão euclidiana, temos que $c'_0 = c_0$ e $q' = q$. Como $q \in S$, temos garantida a unicidade de c_1, \dots, c_n , logo $m = n$ e $c'_i = c_i$ para todo $i = 1, \dots, n$. Portanto $c \in S$, contradição.

Com isto provamos que $S' = \emptyset$. □

A expressão $a = c_0 + c_1 \cdot b + \cdots + c_n \cdot b^n$ com $0 \leq c_i < b$ para $i = 0, \dots, n$, é chamada de *expansão b-ádica* do inteiro a . Analisando com cuidado a demonstração acima obtemos o seguinte algoritmo para calcular a expansão b-ádica de um inteiro não negativo a ,

$$a = bq_0 + c_0 \quad , \quad 0 \leq c_0 < b$$

$$q_0 = bq_1 + c_1 \quad , \quad 0 \leq c_1 < b$$

⋮

$$q_{n-2} = bq_{n-1} + c_{n-1} \quad , \quad 0 \leq c_{n-1} < b \text{ e } q_{n-1} < b.$$

Pondo $c_n = q_{n-1}$, temos que

$$a = c_0 + c_1 \cdot b + \cdots + c_n \cdot b^n$$

Exemplo: Vamos determinar a expansão b -ádica de 723, onde $b = 5$:

$$\begin{aligned} 723 &= 144 \cdot 5 + 3 \\ 144 &= 28 \cdot 5 + 4 \\ 28 &= 5 \cdot 5 + 3 \\ 5 &= 1 \cdot 5 + 0 \quad (1 < 5) \end{aligned}$$

$$\text{logo } 723 = 3 + 4 \cdot 5 + 3 \cdot 5^2 + 0 \cdot 5^3 + 1 \cdot 5^4.$$

O sistema de numeração de base $b > 1$ obtém-se escolhendo um conjunto com b símbolos

$$S = \{s_0, \dots, s_{b-1}\},$$

com $s_0 = 0$, que representam os inteiros de 0 a $b - 1$ e representando um inteiro não negativo s como

$$s = x_n x_{n-1} \cdots x_0,$$

com $x_i \in S$, $i = 0, \dots, n$. Identificam-se

$$0x_n x_{n-1} \dots x_0 \quad \text{e} \quad x_n x_{n-1} \dots x_0$$

(em qualquer sistema de numeração os zeros à esquerda são desprezados). Os inteiros negativos são representados pelos inteiros positivos precedidos do sinal $(-)$.

A justificativa da validade da representação acima se apoia no Teorema 7 que nos garante ser uma bijeção a função

$$\begin{aligned} \mathbb{Z}_b^+ &\longrightarrow \mathbb{Z}^+ \\ x_n \dots x_0 &\longrightarrow c_0 + \cdots + c_n \cdot b^n \end{aligned}$$

onde \mathbb{Z}_b^+ é o conjunto dos elementos da forma $x_n \dots x_0$, com $x_n \neq 0$ se $n > 1$ e onde para cada i , tem-se que c_i é o inteiro correspondente ao símbolo x_i .

No sistema de base 10 usualmente toma-se

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Se $b \leq 10$, utilizam-se os símbolos $0, 1, \dots, b - 1$ e se $b > 10$ utilizam-se os símbolos $0, 1, \dots, 9$ e se introduzem símbolos adicionais para representar $10, \dots, b - 1$.

Problemas

3.1 Mostre que o algarismo das unidades do quadrado de um inteiro no sistema decimal só pode ser 0,1,4,5,6 ou 9.

3.2 Um certo número de três algarismos no sistema decimal aumenta de 36 se se invertem os dois algarismos da direita e diminui de 270 se se invertem os dois algarismos da esquerda. O que acontece ao número se se invertem os dois algarismos extremos?

3.3 Prove que é válida a seguinte regra para calcular o quadrado de um número no sistema decimal cujo algarismo das unidades é 5:

$$(\overline{n} \ 5)^2 = \overline{n(n+1)}25,$$

onde a notação $\overline{x} \ y$ significa o número $x \cdot 10^r + y$, onde r é o número de algarismos de y . Calcule mentalmente os quadrados de 25,45,95 e 105.

3.4 Escolha um número de três algarismos abc no sistema decimal de modo que os algarismos das centenas e o das unidades difiram de pelo menos duas unidades, isto é, $|a - c| \geq 2$. Considere o número $xyz = |abc - cba|$ e efetue a soma de xyz com zyx . O resultado é 1089.

- Justifique o fato de que o resultado independe do número inicialmente escolhido;
- O que aconteceria se os algarismos das unidades e o das centenas diferissem de uma unidade? E se fossem iguais?

3.5 Seja dado o número 5283 na base 10, escreva-o nas bases 2,3,4,5,8 e 15.

3.6 O número 6232 está escrito na base 7, escreva-o na base 5.

3.7 Escreva a tabuada da base 5. Dados os números $a = 23142$ e $b = 43210$ na base 5, ache por meio de um algoritmo os números $a + b$, $b - a$ e $a \cdot b$.

3.8 Por meio de um algoritmo análogo ao usado na base 10, efetue as seguintes operações na base 2

- | | |
|----------------------|------------------------|
| a) $1011 + 1101$ | b) $10011 + 11101101$ |
| c) 1101×110 | d) 101100×101 |

3.9

- a) Considere 36 na base 10, em que base será representado por 51?
- b) Idem para 73 e 243;
- c) Idem para 73 e 242;
- d) Considere o número 21378 na base 9, escreva-o na base 7.

3.10 Utilizando os sistemas decimal e binário, justifique o seguinte algoritmo utilizado pelos antigos egípcios para efetuar a multiplicação de dois inteiros positivos a e b representados no sistema decimal. Ponha a e b no alto de duas colunas. Abaixo de a ponha o quociente q_1 da divisão de a por 2, abaixo de q_1 ponha o quociente q_2 da divisão de q_1 por 2, etc. Abaixo de b ponha $2b$, abaixo de $2b$ ponha $4b$, etc. Toda vez que o número na coluna do a for ímpar, coloque um sinal $+$ ao lado do número da mesma linha na coluna do b . Some todos os números assinalados com $+$, este é o produto de a por b . Exemplo $a = 35$ e $b = 47$:

$$\begin{array}{r}
 35 & 47 & + \\
 17 & 94 & + \\
 8 & 188 \\
 4 & 376 \\
 2 & 752 \\
 1 & 1504 & + \\
 \hline
 1645 & = 35 \times 47.
 \end{array}$$

4. Euclides

Euclides foi um eminente matemático grego. Presume-se que tenha

vivido de 330 a 275 A.C. na cidade de Alexandria, durante o reinado de Ptolomeu I. A contribuição de Euclides à matemática foi considerável, tendo sido o primeiro matemático a apresentar a Geometria e a Aritmética como ciências dedutivas. Sua principal obra são os *Elementos*, um conjunto de treze livros onde é exposta de maneira sistemática e primorosa a matemática de sua época. Partindo de definições, postulados e axiomas e com regras lógicas bem determinadas, as proposições são demonstradas. Este método foi tão marcante que é utilizado até hoje para expôr a matemática.

A Aritmética de Euclides tem início no livro VII dos Elementos, onde é usada sistematicamente sem menção explícita e sem demonstração, a divisão com resto que denominamos de Divisão Euclidiana (Teorema 6).

A Álgebra dos Inteiros

Como num anel nem sempre é possível dividir um elemento por outro, a noção de divisibilidade assume um papel importante. O conceito de máximo divisor comum é natural neste contexto e se relaciona com objetos algébricos chamados ideais. Neste capítulo introduzimos estes conceitos e deduzimos algumas relações entre eles. Em particular, mostramos, como consequência da divisão euclidiana nos inteiros, que do ponto de vista da complexidade dos seus ideais, o anel dos inteiros tem uma estrutura bem simples, fato este que tem consequências algébricas notáveis. Por exemplo, em um anel com estrutura de ideais semelhante à dos inteiros, temos garantida a existência de máximo divisor comum e os seus elementos possuem a propriedade de fatoração única. Esta última propriedade no anel dos inteiros é chamada de Teorema Fundamental da Aritmética e já se encontra parcialmente nos Elementos de Euclides.

1. Divisibilidade

Sejam a e b elementos de um anel A . Se existir um elemento c de A tal que $b = a \cdot c$, diremos que a divide b . Neste caso diremos também que a é *um divisor de b*, ou que b é *um múltiplo de a*, ou ainda que b é *divisível por a*.

A afirmação, a divide b , será simbolizada por $a | b$ e a sua negação por $a \nmid b$.

Num anel A a divisibilidade goza das seguintes propriedades

Proposição 1. *Sejam $a, b, c, d, b_1, \dots, b_n$ elementos de A . As seguin-*

tes afirmações são verdadeiras.

- (i) $a|0$ e $a|a$;
- (ii) Se $a|b$ e $b|c$, então $a|c$;
- (iii) Se $a|b$ e $c|d$, então $a \cdot c|b \cdot d$;
- (iv) Se $a|(b+c)$ e $a|b$, então $a|c$;
- (v) Se $a|b_1, \dots, a|b_n$, então $a|(c_1 \cdot b_1 + \dots + c_n \cdot b_n)$,
 $\forall c_1, \dots, c_n \in A$;
- (vi) Se u é invertível em A , então $u|a$ para todo a .

Demonstração: i. $a|0$ pois $0 = a \cdot 0$ e $a|a$ pois $a = a \cdot 1$.

ii. Se $a|b$ e $b|c$, existem elementos f e g de A tais que $b = a \cdot f$ e $c = b \cdot g$. Segue daí que $c = a \cdot f \cdot g$, logo $a|c$.

iii. Se $a|b$ e $c|d$, existem elementos f e g de A tais que $b = a \cdot f$ e $d = c \cdot g$. Segue daí que $b \cdot d = a \cdot f \cdot c \cdot g = a \cdot c \cdot f \cdot g$ e portanto $a \cdot c|b \cdot d$.

iv. Se $a|(b+c)$ e $a|b$, existem elementos f e g de A tais que $b+c = a \cdot f$ e $b = a \cdot g$. Segue daí que $c = a \cdot f - b = a \cdot f - a \cdot g = a(f-g)$, logo $a|c$.

v. $a|b_i$ significa que existe $d_i \in A$ tal que $b_i = a \cdot d_i$, portanto $c_1 \cdot b_1 + \dots + c_n \cdot b_n = a(c_1 \cdot d_1 + \dots + c_n \cdot d_n)$ e consequentemente $a|(c_1 \cdot b_1 + \dots + c_n \cdot b_n)$.

vi. Seja u um elemento invertível de A , logo $a = u(u^{-1} \cdot a)$ e portanto $u|a$.

Proposição 2. Sejam A um domínio de integridade e $a, b \in A$. Temos que $a|b$ e $b|a$ se, e somente se, existe um elemento invertível u de A tal que $b = u \cdot a$.

Demonstração: Se $a|b$ e $b|a$, então existem elementos u e v de A tais que $b = a \cdot u$ e $a = b \cdot v$, logo $b = b \cdot v \cdot u$ e portanto $b \cdot 1 = b \cdot v \cdot u$. Se $b \neq 0$, pela lei do cancelamento (Proposição 3, Capítulo 2), segue que $1 = v \cdot u$, logo u é invertível. Como $b = a \cdot u$, o resultado segue. Se $b = 0$, de $b|a$ segue que $a = 0$ e neste caso vale também o resultado já que $b = 1 \cdot a$.

Reciprocamente, se $b = u \cdot a$, então $a | b$. Se u é invertível, então $u^{-1} \cdot b = a$ e consequentemente, $b | a$. \square

Corolário. Se a e b são inteiros tais que $a | b$ e $b | a$, então $a = b$ ou $a = -b$.

Demonstração: Pela proposição acima, segue que $b = u \cdot a$ com u invertível em \mathbb{Z} , logo pela Proposição 6, Capítulo 2, tem-se que $u = 1$ ou $u = -1$. \square

Dois elementos a e b de um anel A são ditos *associados* se existir um elemento invertível u de A tal que $a = u \cdot b$.

A noção de elementos associados é fundamental pois no que diz respeito à divisibilidade, dois elementos associados comportam-se exatamente do mesmo modo (veja Problema 1.2).

A relação binária, a é associado de b , em A é uma relação de equivalência em A (veja Problema 1.1).

A Proposição 2 nos diz que num domínio de integridade, a e b são associados se e somente se $a | b$ e $b | a$.

Proposição 3. Se a e b são inteiros com $b \neq 0$ e $a | b$, então $|a| \leq |b|$.

Demonstração: Se $a | b$, então existe um inteiro c tal que $b = a \cdot c$. Como $b \neq 0$, segue que $c \neq 0$, logo pelo Corolário 2 da Proposição 5, Capítulo 2, temos que

$$|b| = |a \cdot c| \geq |a|. \quad \square$$

Sejam a_1, \dots, a_s elementos de um anel A . Diremos que $d \in A$ é um *máximo divisor comum* (mdc) de a_1, \dots, a_s , se as seguintes condições são verificadas.

- (i) O elemento d é um divisor comum de a_1, \dots, a_s
- (ii) Para todo elemento $c \in A$ que divide a_1, \dots, a_s , temos que c divide d .

Com este grau de generalidade, não podemos garantir a existência de um mdc de elementos de A . Antes de discutirmos o problema da existência de mdc, o que será feito na próxima seção, vejamos que

relações guardam entre si, quando existem, os vários máximos divisores comuns de dados elementos de A .

Proposição 4. *Seja d um mdc de a_1, \dots, a_s . Temos que d' é um mdc destes elementos se e somente se $d | d'$ e $d' | d$.*

Demonstração: Suponha que d e d' sejam dois máximos divisores comuns de a_1, \dots, a_s . Logo pelo item (i) da definição acima, temos que d e d' são divisores de a_1, \dots, a_s e portanto pelo item (ii) da definição, segue que $d | d'$ e $d' | d$.

Reciprocamente, suponha que d seja um mdc de a_1, \dots, a_s e que $d | d'$ e $d' | d$. Como $d | a_i$ para todo $i = 1, \dots, s$ e $d' | d$, segue do item (ii) da Proposição 1, que $d' | a_i$ para todo $i = 1, \dots, s$. Seja agora $c \in A$ um divisor comum de a_1, \dots, a_s , logo pelo item (ii) da definição, temos que $c | d$ e como $d | d'$, segue novamente do item (ii) da Proposição 1 que $c | d'$. Temos portanto que d' é um mdc de a_1, \dots, a_s . \square

Corolário. *Num domínio de integridade dois máximos divisores comuns de dados elementos são associados e todo associado de um mdc destes elementos é também um mdc deles.*

Demonstração: Este resultado é uma consequência direta das Proposições 2 e 4. \square

Em particular, quando $A = \mathbb{Z}$, o corolário acima e o corolário da Proposição 2 nos garantem que se d é um mdc de certos inteiros, então $-d$ também o é, e estes são os seus únicos máximos divisores comuns. Portanto, se existir um mdc não nulo dos inteiros a_1, \dots, a_s , existirão dois, um positivo e outro negativo. Usaremos a notação $\text{mdc}(a_1, \dots, a_s)$ para representar o mdc positivo de a_1, \dots, a_s o qual será chamado de “o máximo divisor comum”. Se c é um divisor comum de inteiros a_1, \dots, a_s não todos nulos, então $c \neq 0$, $\text{mdc}(a_1, \dots, a_s) \neq 0$ e $c | \text{mdc}(a_1, \dots, a_s)$, logo pela Proposição 3 temos que

$$c \leq |c| \leq \text{mdc}(a_1, \dots, a_s),$$

e portanto o máximo divisor comum de dados inteiros não todos nulos é o maior dos divisores comuns destes inteiros.

Um elemento m de um anel A é um *mínimo múltiplo comum* (mmc) de elementos a_1, \dots, a_s se são verificadas as seguintes condições

- (i) O elemento m é múltiplo comum de a_1, \dots, a_s ;
- (ii) Para todo elemento $c \in A$ que é múltiplo de a_1, \dots, a_s , temos que $m | c$.

Nesta situação prova-se também que, num domínio de integridade, dois mínimos múltiplos comuns de dados elementos são associados e que todo associado de um mmc destes elementos é também um mmc deles (veja Problema 1.10). Segue então que se existir um mmc não nulo de inteiros a_1, \dots, a_s , existirão dois, um positivo e outro negativo. O mmc positivo será denotado por $\text{mmc}(a_1, \dots, a_s)$ e será chamado de *o mínimo múltiplo comum*. Se c é um múltiplo comum positivo de a_1, \dots, a_s , temos que $\text{mmc}(a_1, \dots, a_s) | c$, logo pela Proposição 3 segue que

$$\text{mmc}(a_1, \dots, a_s) \leq c.$$

Portanto o mmc de dados elementos não nulos é o menor dos múltiplos comuns positivos destes elementos.

Problemas

1.1 Mostre que num anel qualquer, a relação de associado entre elementos é de equivalência.

1.2 Sejam a e b elementos de um anel. Mostre que são equivalentes as afirmações

- (i) a divide b ;
- (ii) todo associado de a divide todo associado de b ;
- (iii) existe um associado de a que divide um associado de b .

1.3 Sejam a, b e c elementos de um domínio de integridade com $c \neq 0$. Mostre que $a | b$ se e somente se $a \cdot c | b \cdot c$.

1.4 Seja n um número inteiro positivo ímpar. Mostre que a soma de n termos consecutivos de uma progressão aritmética com elementos em \mathbb{Z} é divisível por n .

1.5 Dados n números naturais consecutivos, mostre que um e apenas um destes números é divisível por n .

1.6 Sejam m e n inteiros ímpares. Mostre que

- a) $8 \mid (m^2 - n^2)$
- b) $8 \mid (m^4 + n^4 - 2)$

1.7 Mostre que para todo inteiro não negativo n , tem-se que

$$9 \mid (10^n + 3 \cdot 4^{n+2} + 5)$$

Sugestão: Por indução sobre n .

1.8 Sejam A um anel, a e b elementos de A e n um número natural. Mostre que

- a) Para todo n tem-se que $(a - b) \mid (a^n - b^n)$;
- b) Para todo n ímpar tem-se que $(a + b) \mid (a^n + b^n)$;
- c) Para todo n par tem-se que $(a + b) \mid (a^n - b^n)$.

Sugestão: Mostre que, para todos os números naturais n e m , valem as identidades:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2} \cdot b + \dots + a \cdot b^{n-2} + b^{n-1})$$

$$a^{2m+1} + b^{2m+1} = (a + b)(a^{2m} - a^{2m-1}b + \dots - ab^{2m-1} + b^{2m})$$

$$a^{2m} - b^{2m} = (a + b)(a^{2m-1} - a^{2m-2}b + \dots + ab^{2m-2} - b^{2m-1})$$

1.9 Mostre que para todo número inteiro positivo n , tem-se que

- a) $9 \mid (10^n - 1)$
- b) $3 \mid (10^n - 7^n)$
- c) $8 \mid (3^{2n} - 1)$
- d) $6 \mid (5^{2n+1} + 1)$
- e) $17 \mid (10^{2n+1} + 7^{2n+1})$
- f) $19 \mid (3^{2n+1} + 4^{4n+2})$
- g) $6 \mid (5^{2n} - 1)$
- h) $13 \mid (9^{2n} - 4^{2n})$
- i) $53 \mid (7^{4n} - 2^{4n})$

1.10 Seja A um domínio de integridade. Mostre que

- a) dois mínimos múltiplos comuns de dados elementos são associados;
- b) se um elemento é associado de um mmc de dados elementos, ele também é um mmc destes elementos.

1.11 a) Mostre que 0 é um mdc de a_1, \dots, a_s se e somente se $a_i = 0$ para todo $i = 1, \dots, s$;

b) Mostre que 0 é um mmc de a_1, \dots, a_s se e somente se $a_i = 0$ para algum $i = 1, \dots, s$.

2. Ideais

A definição de ideal foi introduzida no final do século passado por Dedekind a fim de estudar certas questões em Teoria dos Números. Esta noção tornou-se um objeto central na teoria dos anéis. Nesta seção teremos a oportunidade de ver como esta noção se relaciona com as noções de máximo divisor comum e de mínimo múltiplo comum.

Um subconjunto I de um anel A será chamado de *ideal* de A se possuir as seguintes propriedades:

- (i) $I \neq \emptyset$;
- (ii) Se $a, b \in I$, então $a + b \in I$;
- (iii) Se $a \in A$ e $b \in I$, então $a \cdot b \in I$.

Das propriedades (i) e (iii) segue claramente que $0 \in I$. Note que da definição segue que $I = \{0\}$ é um ideal de A . Este ideal será chamado de ideal nulo e será simbolizado por (0) .

Da propriedade (iii) da definição segue que se $a \in I$, então $-a = (-1) \cdot a \in I$. Disto e de (ii) segue que se $a, b \in I$, então $a - b \in I$.

Das propriedades (ii) e (iii) temos que se $a_1, \dots, a_s \in I$ e $n_1, \dots, n_s \in A$, então $n_1 \cdot a_1 + \dots + n_s a_s \in I$.

Exemplos

1. Seja $a \in A$. Definimos $I(a) = \{n \cdot a \mid n \in A\}$. É fácil verificar (faça-o) que $I(a)$ é um ideal de A . Neste caso, diremos que o ideal $I(a)$ é gerado por a ou que a é um gerador do ideal $I(a)$. Por exemplo, se $A = \mathbb{Z}$, então o ideal gerado por 2 é o conjunto dos números inteiros pares e o ideal gerado por 1 é todo \mathbb{Z} .

2. Sejam $a, b \in A$. Definimos

$$I(a, b) = \{n \cdot a + m \cdot b \mid m, n \in A\}$$

É também fácil verificar que $I(a, b)$ é um ideal de A . Neste caso, diremos que o ideal $I(a, b)$ é gerado por a e b ou que a e b são geradores de $I(a, b)$.

3. Mais geralmente, sejam $a_1, \dots, a_s \in A$, definimos

$$I(a_1, \dots, a_s) = \{n_1 \cdot a_1 + \dots + n_s \cdot a_s \mid n_1, \dots, n_s \in A\}.$$

Este conjunto é um ideal de A , ideal este gerado por a_1, \dots, a_s . É claro que $a_i \in I(a_1, \dots, a_s)$ para todo $i = 1, \dots, s$.

Um ideal I de um anel A que é da forma $I(a)$ para algum $a \in A$ será chamado de *ideal principal*.

Lema 1. *Dados um ideal J de A e $a_1, \dots, a_s \in A$, temos que*

$$I(a_1, \dots, a_s) \subset J \text{ se e somente se } a_1, \dots, a_s \in J.$$

Demonstração: (\Rightarrow) Como $a_1, \dots, a_s \in I(a_1, \dots, a_s) \subset J$, segue que $a_1, \dots, a_s \in J$.

(\Leftarrow) Suponha que $a_1, \dots, a_s \in J$. Como J é um ideal de A , temos que $n_1 \cdot a_1 + \dots + n_s \cdot a_s \in J$ para todos os n_1, \dots, n_s em A , logo $I(a_1, \dots, a_s) \subset J$. \square

Note que o Lema 1 nos diz que $I(a_1, \dots, a_s)$ é o menor ideal de A que contém $\{a_1, \dots, a_s\}$.

Lema 2. *Sejam $a_1, \dots, a_s \in A$. Valem as seguintes igualdades:*

- (i) $I(a_1, \dots, a_s, 0) = I(a_1, \dots, a_s)$;
- (ii) $I(a_1, \dots, a_i, \dots, a_j, \dots, a_s) = I(a_1, \dots, a_j, \dots, a_i, \dots, a_s)$;
- (iii) *Quaisquer que sejam u_1, \dots, u_s elementos invertíveis de A ,*

$$I(u_1 \cdot a_1, \dots, u_s \cdot a_s) = I(a_1, \dots, a_s)$$

- (iv) *Para todo t em A ,*

$$I(a_1, \dots, a_{s-1}, a_s) = I(a_1, \dots, a_{s-1}, a_s - t \cdot a_{s-1})$$

Demonstração: i. e ii. são imediatas.

iii. Em vista do Lema 1, basta mostrar que $u_1 \cdot a_1, \dots, u_s \cdot a_s$ pertencem a $I(a_1, \dots, a_s)$, o que é óbvio; e que a_1, \dots, a_s pertencem a $I(u_1 \cdot a_1, \dots, u_s \cdot a_s)$, o que segue das igualdades

$$a_i = 1 \cdot a_i = (u_i^{-1} \cdot u_i) \cdot a_i = u_i^{-1} \cdot (u_i \cdot a_i),$$

e do fato de que o último membro destas igualdades pertence a $I(u_1 \cdot a_1, \dots, u_s \cdot a_s)$.

iv. Pelo Lema 1 é claro que

$$I(a_1, \dots, a_{s-1}, a_s - t \cdot a_{s-1}) \subset I(a_1, \dots, a_{s-1}, a_s).$$

Por outro lado,

$$a_s = (a_s - t \cdot a_{s-1}) + t \cdot a_{s-1} \in I(a_1, \dots, a_{s-1}, a_s - t \cdot a_{s-1}),$$

e a outra inclusão segue novamente do Lema 1. \square

Exemplos: Seja $A = \mathbb{Z}$. Aplicando o Lema 2 repetidas vezes, temos

$$1) I(2, 3) = I(2, 3 - 1 \cdot 2) = I(2, 1) = I(1, 2 - 2 \cdot 1) = I(1, 0) = I(1) = \mathbb{Z}$$

$$2) I(4, 6) = I(4, 6 - 4 \cdot 1) = I(4, 2) = I(2, 4) = I(2, 4 - 2 \cdot 2) = I(2, 0) = I(2)$$

$$3) I(a, b) = I(-a, b) = I(a, -b) = I(-a, -b) = I(|a|, |b|).$$

A variedade dos tipos de ideais de um anel, de certo modo mede a complexidade do anel. O anel dos inteiros é bastante simples deste ponto de vista como mostra o seguinte teorema, consequência da existência da divisão euclidiana em \mathbb{Z} .

Teorema 1. *Dado um ideal $I \neq (0)$ de \mathbb{Z} , temos que $I = I(d)$ onde $d = \min(I \cap \mathbb{N})$.*

Demonstração: Seja $I \neq (0)$ um ideal de \mathbb{Z} . O conjunto $I \cap \mathbb{N}$ é não vazio. De fato, existe $a \neq 0$ em I , como a e $-a$ são elementos de I , segue que $I \cap \mathbb{N} \neq \emptyset$. Como $I \cap \mathbb{N}$ é limitado inferiormente, pelo Princípio de Boa Ordenação ele admite um menor elemento d . Vamos agora provar que $I = I(d)$.

É claro pelo Lema 1 que $I(d) \subset I$. Por outro lado, seja x um elemento de I . Pela divisão euclidiana em \mathbb{Z} , existem q e r em \mathbb{Z} tais que $x = d \cdot q + r$ com $0 \leq r < d$. Suponha que $r \neq 0$, logo

$r = x - d \cdot q \in I \cap \mathbb{N}$, o que contradiz o fato de d ser o menor elemento de $I \cap \mathbb{N}$ e portanto $r = 0$. Consequentemente $x = d \cdot q \in I(d)$, o que prova que $I \subset I(d)$. Está portanto provado que $I = I(d)$. \square

Um domínio de integridade A tal que todo ideal é principal é chamado de *domínio principal*. O teorema acima nos diz que \mathbb{Z} é um domínio principal. Este teorema é um típico teorema de existência, não fornecendo nenhum método para o cálculo do gerador d do ideal. O cálculo efetivo de d será abordado no próximo capítulo.

Proposição 5. *Sejam A um anel e a e b elementos de A . valem as seguintes afirmações:*

- (i) *$I(a) = I(b)$ se e somente se $a | b$ e $b | a$;*
- (ii) *Se A é um domínio de integridade, então $I(a) = I(b)$ se e somente se a e b são associados;*
- (iii) *Suponha $A = \mathbb{Z}$. Temos que $I(a) = I(b)$ se e somente se $a = \pm b$.*

Demonstração: i. Do Lema 1 temos que $I(b) \subset I(a)$ e $I(a) \subset I(b)$ se e somente se $b \in I(a)$ e $a \in I(b)$ e isto por sua vez é equivalente a $a | b$ e $b | a$.

ii. Esta afirmação segue de (i) e da Proposição 2.

iii. Esta afirmação segue de (ii) e do fato que os elementos invertíveis de \mathbb{Z} são 1 e -1 (veja Proposição 6, Capítulo 2). \square

Segue do Teorema 1 e do item (iii) da Proposição 5, que todo ideal não nulo de \mathbb{Z} tem exatamente dois possíveis geradores, um positivo e outro negativo. O gerador positivo do ideal $I(a_1, \dots, a_s)$ será simbolizado por (a_1, \dots, a_s) .

Proposição 6. *Sejam A um anel e a_1, \dots, a_s elementos de A . Se $d \in A$ é tal que $I(a_1, \dots, a_s) = I(d)$, então d é um mdc de a_1, \dots, a_s .*

Demonstração: Temos por hipótese que $I(a_1, \dots, a_s) = I(d)$, logo $a_1, \dots, a_s \in I(d)$ e portanto $d | a_1, \dots, d | a_s$.

Suponha agora que c seja um divisor de a_1, \dots, a_s , logo $I(d) = I(a_1, \dots, a_s) \subset I(c)$, portanto $d \in I(c)$ e consequentemente $c | d$.

Isto prova que d é um mdc de a_1, \dots, a_s . \square

A proposição acima admite os seguintes corolários cujas demonstrações são imediatas e por isso serão omitidas.

Corolário 1. *Sejam A um domínio principal e a_1, \dots, a_s elementos de A . Então existe um mdc destes elementos e todo mdc é da forma $n_1 \cdot a_1 + \dots + n_s \cdot a_s$ para alguns elementos $n_1, \dots, n_s \in A$.*

Corolário 2. *Dados $a_1, \dots, a_s \in \mathbb{Z}$, existe o mdc destes elementos e temos $\text{mdc}(a_1, \dots, a_s) = (a_1, \dots, a_s)$.*

A seguir utilizaremos indistintamente em \mathbb{Z} as notações $\text{mdc}(a_1, \dots, a_s)$ e (a_1, \dots, a_s) .

Problemas

2.1 Sejam A um anel e I um ideal de A . Mostre que:

- a) $I = A$ se e somente se I contém um elemento invertível de A ;
- b) A é um corpo se e somente se os seus únicos ideais são (0) e o próprio A .

2.2 Supondo $A = \mathbb{Z}$ e $n \in \mathbb{Z}$, mostre que

- a) $I(2, 3) = \mathbb{Z}$
- b) $I(n, n+1) = \mathbb{Z}$
- c) $I(n, n^2 + 1) = \mathbb{Z}$

2.3 Mostre que todo subconjunto I não vazio de \mathbb{Z} fechado para a subtração é um ideal.

Sugestão: Para mostrar que $n \cdot a \in I$ para todo n em \mathbb{Z}^+ e a em I , use indução matemática.

2.4 Sejam a, b, a', b', m, n, r e s inteiros tais que $m \cdot s - n \cdot r = \pm 1$, $a' = m \cdot a + n \cdot b$ e $b' = r \cdot a + s \cdot b$, mostre que $I(a, b) = I(a', b')$.

2.5 Sejam I e J ideais de um anel A . Mostre que

- a) $I \cap J$ é um ideal de A ;
- b) $I + J = \{x + y \mid x \in I, y \in J\}$ é um ideal de A ;
- c) $I + J = I$ se e somente se $J \subset I$.

2.6 Mostre que se $a_1, \dots, a_s \in \mathbb{Z}$, então

- a) $I(a_1, \dots, a_s) = I(a_1) + \dots + I(a_s);$
 b) $(a_1, \dots, a_{s-2}, a_{s-1}, a_s) = (a_1, \dots, a_{s-2}, (a_{s-1}, a_s))$

Observação: Esta última fórmula permite calcular o mdc de vários inteiros iteradamente, sabendo calcular o mdc de dois elementos.

2.7 Seja $(I_n)_{n \in \mathbb{N}}$ uma família de ideais de um anel A . Mostre que

- a) $\bigcap_{n \in \mathbb{N}} I_n$ é um ideal de A ;
 b) Se $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$, então $\bigcup_{n \in \mathbb{N}} I_n$ é um ideal de A .

2.8 Sejam A um anel e a_1, \dots, a_s elementos não nulos de A . Mostre que se o ideal $I(a_1) \cap \dots \cap I(a_s)$ (veja Problema 2.5(a) ou Problema 2.7(a)) é gerado por um elemento m de A , então m é um mmc de a_1, \dots, a_s . Conclua que num domínio principal, sempre existe um mmc de dados elementos. Mostre que se $A = \mathbb{Z}$, então

$$\text{mmc}(a_1, \dots, a_s) = \min(I(a_1) \cap \dots \cap I(a_s) \cap \mathbb{N}).$$

2.9 Sejam a_1, \dots, a_s e n inteiros. Mostre que

$$(n \cdot a_1, \dots, n \cdot a_s) = |n| \cdot (a_1, \dots, a_s).$$

3. Fatoração

Um elemento não nulo e não invertível de um anel é dito *irredutível* se os seus únicos divisores são os elementos invertíveis do anel e os seus próprios associados. Um elemento não irredutível será dito *redutível*. Note que todo associado de um elemento irredutível (respectivamente, redutível) é também irredutível (respectivamente, redutível).

Exemplos

- O número 2 é irredutível em \mathbb{Z} , pois os seus únicos divisores são ± 1 e ± 2 .
- O número 4 não é irredutível em \mathbb{Z} pois $2 \mid 4$ e 2 não é invertível nem associado de 4.

O lema que segue será útil na demonstração da próxima proposição

Lema 3. *Num domínio principal A , toda cadeia ascendente de ideais*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

é estacionária; isto é, existe um índice m tal que

$$I_m = I_{m+1} = \cdots$$

Demonstração: Verifica-se facilmente que

$$\bigcup_{j \geq 1} I_j$$

é um ideal de A (veja Problema 2.7). Como A é um domínio principal, existe $a \in A$ tal que

$$\bigcup_{j \geq 1} I_j = I(a).$$

Segue daí que

$$a \in \bigcup_{j \geq 1} I_j$$

e portanto $a \in I_m$ para algum m . Portanto $a \in I_n$ para todo $n \geq m$ e consequentemente $I(a) \subset I_n$ para todo $n \geq m$. Como para todo n , temos que

$$I_n \subset \bigcup_{j \geq 1} I_j = I(a),$$

segue que $I_n = I(a)$ para todo $n \geq m$. □

Proposição 7. *Todo elemento não nulo e não invertível de um domínio principal possui pelo menos um divisor irreduzível.*

Demonstração: Sejam A um domínio principal e a um elemento de A não nulo e não invertível. Se a é irreduzível, nada temos a provar. Suponha agora que a seja redutível, logo pela definição, a tem um divisor a_1 que não é invertível nem associado de a , portanto

$$I(a) \subsetneq I(a_1) \subsetneq A,$$

onde $I(a) \neq I(a_1)$ pois a e a_1 não são associados (veja Proposição 5, (ii)) e $I(a_1) \neq A$ pois a_1 é não invertível (justifique).

Se a_1 é irreduzível, o resultado fica estabelecido. Se a_1 é reduzível, ele possui um divisor a_2 que não é invertível nem é associado de a_1 , logo temos que

$$I(a) \subsetneq I(a_1) \subsetneq I(a_2) \subsetneq A.$$

E assim sucessivamente até que, ou para algum n temos que a_n é irreduzível e portanto é um divisor irreduzível de a , ou temos uma cadeia infinita de ideais

$$I(a) \subsetneq I(a_1) \subsetneq I(a_2) \subsetneq \cdots \subsetneq I(a_n) \subsetneq \cdots,$$

o que não é possível tendo em vista o Lema 3. \square

Um domínio de integridade A é um *domínio de fatoração única* (DFU), se todo elemento não nulo e não invertível de A se fatora como produto de um número finito de elementos irreduzíveis. Além disso, tal fatoração é única a menos da ordem dos fatores e de elementos associados, isto é, se $p_1, \dots, p_n, q_1, \dots, q_m$ são elementos irreduzíveis de A e se

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

então $n = m$ e após um reordenamento de q_1, \dots, q_n , se necessário, temos que p_i e q_i são associados para todo $i = 1, \dots, n$.

Todo corpo, por ter todos os seus elementos não nulos invertíveis, é um DFU (pela vacuidade da condição de fatoração).

Um elemento a não nulo e não invertível de um anel A é dito *primo*, se toda vez que a divide o produto de dois elementos de A , ele divide um dos fatores. Vê-se facilmente que se a é primo, então todo associado de a é primo.

Exemplos

1. O número 2 é primo em \mathbb{Z} . De fato, se $2 | b \cdot c$, então b ou c tem que ser par (pois o produto de dois números ímpares é ímpar).
2. O número 3 é primo em \mathbb{Z} . De fato, suponha que $3 | b \cdot c$. Dividindo

b e c por 3 temos que

$$b = 3q_1 + r_1 , \quad c = 3q_2 + r_2,$$

com $0 \leq r_1 < 3$ e $0 \leq r_2 < 3$. Logo

$$b \cdot c = 3(3q_1 \cdot q_2 + q_1 \cdot r_2 + q_2 \cdot r_1) + r_1 \cdot r_2,$$

portanto $3 | r_1 \cdot r_2$. Isto implica em face das desigualdades acima envolvendo r_1 e r_2 que $r_1 \cdot r_2 = 0$, ou seja, $3 | b$ ou $3 | c$.

3. O número 4 não é primo em \mathbb{Z} pois $4 | 2 \cdot 6$ e no entanto, temos que $4 \nmid 2$ e $4 \nmid 6$.

A relação entre elementos primos e irreduutíveis é dada nas três proposições seguintes.

Proposição 8. *Num domínio de integridade, todo elemento primo é irreduutível.*

Demonstração: Seja p um elemento primo de um anel A e suponha que para algum $a \in A$ tenhamos $a | p$. Queremos provar que a é invertível ou que a é um associado de p .

Com efeito, se $a | p$, então $p = a \cdot b$ para algum b . Logo $p | a \cdot b$ e como p é primo, temos que $p | a$ ou $p | b$. Suponhamos inicialmente que $p | a$. Como por hipótese $a | p$, segue da Proposição 2 que a é um associado de p . Em seguida suponhamos que $p | b$. Da igualdade $p = a \cdot b$ segue que $b | p$, logo pela Proposição 2, existe u invertível tal que $p = u \cdot b$. Segue então que $u \cdot b = p = a \cdot b$ e portanto, pela lei do cancelamento, tem-se que $a = u$ e consequentemente a é invertível.

□

Corolário. *Sejam p, p_1, \dots, p_n elementos primos de um domínio de integridade. Se $p | p_1 \cdots p_n$, então p é associado de p_i para algum $i = 1, \dots, n$.*

Demonstração: Se $p | p_1 \cdots p_n$, então pela definição de elemento primo, juntamente com um argumento simples de indução, segue que $p | p_i$ para algum $i = 1, \dots, n$. Agora, como p_i é primo, pela proposição acima ele é irreduutível e como $p | p_i$ e p não é invertível (por ser primo), segue que p é associado de p_i .

□

A recíproca da Proposição 8 nem sempre é verdadeira conforme veremos no Capítulo 10. Entretanto, o resultado pode valer com hipóteses adicionais como se poderá ver na próxima proposição.

Proposição 9. *Num domínio principal, todo elemento irreduzível é primo.*

Demonstração: Seja p um elemento irreduzível de um domínio principal A . Suponha que $p \mid a \cdot b$ e que $p \nmid a$, vamos provar que $p \mid b$.

Com efeito, sendo A principal, existe $c \in A$ tal que $I(a, p) = I(c)$, logo $c \mid a$ e $c \mid p$. Como os únicos divisores de p são os elementos invertíveis de A e os associados de p , segue que c é associado de p ou c é invertível. Note que c não é associado de p pois se fosse, teríamos $p \mid c$ e como $c \mid a$, seguiria então que $p \mid a$, o que é uma contradição. Temos portanto que c é invertível e consequentemente (veja Problema 2.1),

$$I(a, p) = I(c) = A.$$

Segue daí que existem elementos m e n em A tais que

$$1 = n \cdot a + m \cdot p.$$

Multiplicando por b ambos os membros da igualdade acima, temos que

$$b = n \cdot a \cdot b + m \cdot p \cdot b,$$

e como $p \mid a \cdot b$, segue que $p \mid b$; como queríamos demonstrar. \square

Proposição 10. *Em \mathbb{Z} um elemento é primo se e somente se ele é irreduzível.*

Demonstração: Isto decorre das Proposições 8,9 e do fato de \mathbb{Z} ser domínio principal (Teorema 1). \square

Teorema 2. *Todo domínio principal é domínio de fatoração única.*

Demonstração: Sejam A um domínio principal e a um elemento não nulo e não invertível de A . Pela Proposição 7, o elemento a tem pelo menos um divisor irreduzível p_1 , logo existe $a_1 \neq 0$ tal que

$$a = a_1 \cdot p_1.$$

Se a_1 não é invertível, então ele possui um divisor irredutível p_2 , logo

$$a = a_2 \cdot p_2 \cdot p_1.$$

Assim sucessivamente, determinando uma seqüência de pares de elementos (a_i, p_i) com os p_i irredutíveis e tais que $a_i = a_{i+1} \cdot p_{i+1}$. Vamos mostrar que este procedimento tem que parar após um número finito de passos, isto é, para algum n temos que a_n é invertível.

Com efeito, se nenhum dos elementos a_1, \dots, a_n, \dots fosse invertível, teríamos para todo i que $a_{i+1} | a_i$ e a_i não é associado de a_{i+1} , logo teríamos a seguinte cadeia infinita

$$I(a) \subsetneq I(a_1) \subsetneq I(a_2) \subsetneq \dots \subsetneq I(a_n) \subsetneq \dots,$$

o que é absurdo em vista do Lema 3. Portanto, para algum n temos que a_n é invertível. Pondo $a_n = u$, temos que

$$a = p_1 \cdots p_{n-1} \cdot (up_n)$$

com $p_1, \dots, p_{n-1}, up_n$ irredutíveis (portanto, pela Proposição 9, também primos).

Provaremos agora, por indução sobre n , a unicidade de tal escrita. Suponha que $n = 1$ e que

$$p_1 = q_1 \cdots q_m,$$

com p_1, q_1, \dots, q_m irredutíveis (e portanto primos). Como da equação acima segue que $p_1 | q_1 \cdots q_m$, pelo corolário da Proposição 8 temos que p_1 é associado de q_i para algum i . Reordenando os q_j , se necessário, podemos supor que $i = 1$, logo $p_1 = w \cdot q_1$, onde w é invertível. Se $m > 1$, seguiria que

$$w = q_2 \cdots q_m,$$

o que é impossível pois nenhum elemento irredutível pode dividir um elemento invertível (justifique). Portanto $m = 1$ e p_1 é associado de q_1 .

Suponha agora a unicidade válida para $n - 1$ e suponha que

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

com p_1, \dots, p_n e q_1, \dots, q_m irredutíveis, logo primos. Segue que $p_n | q_1 \cdots q_m$ e novamente, pelo Corolário da Proposição 8, temos para algum i que p_n e q_i são associados. Novamente, a menos da reordenação dos q_j podemos supor que $i = m$ e portanto $p_n = w \cdot q_m$ com w invertível. Segue então que

$$w \cdot p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1}.$$

Pela hipótese de indução segue que $n - 1 = m - 1$, portanto $n = m$, e após reordenação dos q_j , se necessário, temos que cada p_i é associado de q_i para todo $i = 1, \dots, n - 1$. Como já mostramos acima que p_n e q_n são associados, fica demonstrada a unicidade no nível n . \square

Corolário 1. *O anel dos inteiros é um Domínio de Fatoração Única.*

Corolário 2 (Teorema Fundamental da Aritmética). *Todo inteiro $a \neq 0, \pm 1$, pode ser escrito sob a forma*

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$

com os p_i números primos positivos distintos e os α_i inteiros positivos. Além disso, esta escrita é única a menos da ordem dos fatores.

Dados dois inteiros quaisquer a e b podemos representá-los do seguinte modo

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n},$$

com p_1, \dots, p_n primos positivos distintos mas com $\alpha_1, \dots, \alpha_n$, β_1, \dots, β_n inteiros positivos ou nulos. Nesta representação poderíamos facilmente mostrar (veja Problema 3.9) que

$$\text{mdc}(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n},$$

com $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, \dots, n$. E que

$$\text{mmc}(a, b) = p_1^{\delta_1} \cdots p_n^{\delta_n},$$

com $\delta_i = \max\{\alpha_i, \beta_i\}$, $i = 1, \dots, n$.

Dois elementos de um anel A são ditos *primos entre si*, se os únicos divisores comuns destes elementos são os elementos invertíveis de A .

Da definição acima segue facilmente que quando $A = \mathbb{Z}$, temos que os elementos a e b de \mathbb{Z} são primos entre si se, e somente se, $(a, b) = 1$. Neste contexto temos que, se

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

e

$$b = \pm q_1^{\beta_1} \cdots q_m^{\beta_m}$$

com p_1, \dots, p_n primos positivos distintos, q_1, \dots, q_m primos positivos distintos e $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ inteiros positivos, então a e b são primos entre si se e somente se $p_i \neq q_j$ para todo i e j .

O seguinte resultado é fundamental.

Proposição 11. *Todo número racional não nulo se escreve de modo único na forma $\frac{a}{b}$ com a e b primos entre si e $b > 0$.*

Demonstração: Represente o número racional como $\frac{a'}{b'}$ com a' e b' inteiros e $b' \neq 0$. Se b' é negativo, transfira o seu sinal para o numerador. Decomponha a' e b' em produtos de primos e simplifique os seus fatores comuns; daí resulta que $\frac{a'}{b'} = \frac{a}{b}$ com $b > 0$ e a e b primos entre si. \square

Proposição 12. *O “número” $\sqrt{2}$ não é racional.*

Demonstração: Suponha por absurdo que $\sqrt{2} = \frac{a}{b}$ com a e b inteiros primos entre si. Desta equação, elevando ambos os membros ao quadrado, obtemos que

$$2b^2 = a^2.$$

Segue daí que $2 | a^2$ e como 2 é primo, devemos ter $2 | a$ e portanto $a = 2 \cdot c$ para algum inteiro c . Temos então que

$$2b^2 = a^2 = 4 \cdot c^2,$$

logo $b^2 = 2c^2$ e portanto $2 | b^2$ e consequentemente $2 | b$. Temos portanto que $2 | a$ e $2 | b$, o que é uma contradição pois a e b são primos entre si. \square

A Proposição 12 com a demonstração que apresentamos se encontra nos Elementos de Euclides. Os Gregos Antigos haviam portanto detectado a existência de “números” que não são racionais. No Capítulo

8 construiremos o corpo dos números reais \mathbb{R} como extensão do corpo \mathbb{Q} dos números racionais onde $\sqrt{2}$ terá o seu lugar.

Problemas

3.1 Mostre que num DFU todo elemento irredutível é primo.

3.2 Sejam A um DFU e a, b e c elementos de A . Suponha a e b primos entre si. Mostre que

- i) Se $a | b \cdot c$, então $a | c$;
- ii) Se $a | c$ e $b | c$, então $a \cdot b | c$.

3.3 Sejam A um domínio principal e a e b elementos de A não ambos nulos. Mostre que são equivalentes a afirmações:

- (i) a e b são primos entre si;
- (ii) a e b possuem um mdc invertível;
- (iii) $I(a, b) = A$;
- (iv) Existem elementos m e n de A tais que $m \cdot a + n \cdot b = 1$.

3.4 Sejam a e b inteiros não ambos nulos. Mostre que

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1$$

3.5 Sejam a, b e c inteiros e m e n naturais. Mostre que

- (i) Se $(a, c) = 1$, então $(a \cdot b, c) = (b, c)$;
- (ii) Se $(a, b) = 1$, então $(a^m, b^n) = 1$.

3.6 Sejam m e n inteiros positivos. Mostre que se $\sqrt[m]{n}$ não é inteiro, então ele é irracional.

3.7 Mostre que se a é um inteiro positivo que não é uma potência de 10, então $\log_{10} a$ é irracional.

3.8 Sejam b e m inteiros com $m > 1$

- (i) Mostre que o número de inteiros divisíveis por m na seqüência $b, 2b, \dots, mb$ é (m, b) ;

- (ii) Se $(m, b) = 1$, mostre que os restos da divisão de $b, 2b, \dots, mb$ por m são os números $0, 1, \dots, m - 1$, em alguma ordem.
- (iii) Se $(m, b) = 1$; mostre que de m termos consecutivos quaisquer de uma progressão aritmética de razão b , um e somente um destes termos é divisível por m .

3.9 Sejam A um DFU, $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = vp_1^{\beta_1} \cdots p_n^{\beta_n}$ com u e v invertíveis, os p_i irreduzíveis dois a dois não associados e $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ inteiros maiores ou iguais a zero. Mostre que $p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ e $p_1^{\delta_1} \cdots p_n^{\delta_n}$ com $\gamma_i = \min\{\alpha_i, \beta_i\}$ e $\delta_i = \max\{\alpha_i, \beta_i\}$, para $i = 1, \dots, n$, são respectivamente um mdc e um mmc de a e b .

3.10 Sejam A um DFU e a e b elementos não nulos de A . Sejam d um mdc e m um mmc de a e b . Mostre que os elementos $m \cdot d$ e $a \cdot b$ são associados. Mostre que em \mathbb{Z} vale a relação

$$\text{mmc}(a, b) = \frac{|a \cdot b|}{\text{mdc}(a, b)}.$$

3.11 Seja p um número primo positivo. Mostre que todo número racional não nulo x se escreve de modo único na forma

$$x = p^n \cdot \frac{a}{b},$$

com $a, b, n \in \mathbb{Z}$, $b > 0$ e $(a, b) = (a, p) = (b, p) = 1$. Define-se o *valor absoluto p-ádico* como segue:

$$|0|_p = 0 \quad \text{e} \quad |x|_p = \frac{1}{p^n}.$$

Mostre que para todo $x, y \in \mathbb{Q}$ e $n \in \mathbb{Z}$ tem-se que

- (i) $|x \cdot y|_p = |x|_p \cdot |y|_p$
- (ii) $|x + y|_p \leq |x|_p + |y|_p$
- (iii) $|n|_p \leq 1$

A Aritmética dos Inteiros

Em Matemática há vários tipos de teoremas de existência. Alguns destes teoremas são de natureza construtiva, isto é, a demonstração da existência de um determinado objeto matemático consiste em exibir um algoritmo que permite, pelo menos em teoria, calculá-lo. Outros, são de natureza mais conceitual, apenas garantindo a existência e eventualmente caracterizando o objeto mas não fornecendo nenhum método para calculá-lo.

O Capítulo anterior contém vários resultados deste último tipo. Por exemplo, o Teorema 1 garante que todo ideal de \mathbb{Z} pode ser gerado por um único elemento e que ainda este elemento pode ser caracterizado como o mínimo de um determinado conjunto, mas a demonstração deste teorema não nos fornece nenhuma indicação de como este elemento pode ser calculado. Este último tipo de prova tornou-se muito popular desde o final do século passado e um dos argumentos a seu favor até muito recentemente era de que mesmo de posse de um algoritmo, a complexidade dos cálculos torna a execução do mesmo impraticável. Com o desenvolvimento recente da Ciência da Computação, aumentando a nossa capacidade computacional, voltou naturalmente o interesse pelos algoritmos.

No presente capítulo estudaremos algumas propriedades específicas dos inteiros, chamadas de propriedades aritméticas, dando ênfase aos aspectos computacionais. Inicialmente, discutiremos algumas questões relativas à distribuição dos números primos que nos conduzem rapidamente a problemas muito difíceis ou a questões ainda em aberto. Em seguida descrevemos o algoritmo de Euclides para o cálculo efetivo do mdc de dois inteiros. Este algoritmo, apesar de sua

idade, continua sendo um dos mais eficientes do ponto de vista computacional para o cálculo do mdc. A questão da eficiência ou “custo” de um determinado algoritmo é central em Computação Científica pois o seu sucesso é função da rapidez com a qual uma máquina pode efetuar os cálculos. Finalmente mostramos como se resolvem certas equações envolvendo inteiros usando o algoritmo de Euclides.

1. Números Primos

Tivemos oportunidade no capítulo anterior de verificar que os números primos são, do ponto de vista da divisibilidade, os mais simples pois são irredutíveis e pelo Teorema Fundamental da Aritmética são suficientes para gerar todos os inteiros diferentes de 0 e ± 1 por meio de multiplicações. A primeira pergunta natural que surge é, quantos são os números primos? A resposta foi dada por Euclides nos Elementos e é a seguinte

Teorema 1 (Euclides). *Em \mathbb{Z} existem infinitos números primos.*

Demonstração: Suponhamos por absurdo que os números primos sejam em número finito. Seja p o maior número primo positivo e considere o número a formado pelo produto de todos os primos positivos diminuído de 1, portanto

$$a = (2 \cdot 3 \cdots p) - 1 \quad (1)$$

Como $a \neq 0, \pm 1$, pelas Proposições 7 e 10 do Capítulo 4, temos que a possui um divisor primo q , que podemos supor positivo. Como q é um número primo positivo, ele é um dos fatores de $2 \cdot 3 \cdots p$, logo de (1) segue que $q | (-1)$, o que é absurdo. \square

O teorema acima é um típico teorema de existência, não nos dando nenhum método para determinar números primos. O problema de determinar números primos continua sem solução satisfatória.

Damos a seguir um método bem antigo para a elaboração de tabelas de números primos até a ordem que se desejar. O método é conhecido pelo nome de *Crivo de Eratósstenes* e se baseia no seguinte resultado

Lema 1. *Se um número inteiro n maior do que 1 não é divisível por*

nenhum primo positivo p tal que $p^2 \leq n$, então ele é primo.

Demonstração: Suponha por absurdo que n não é primo e seja q o menor número primo positivo que divide n (q existe em virtude das Proposições 7,10 do Capítulo 4 e do princípio da boa ordenação em \mathbb{Z}). Temos então que

$$n = q \cdot m \quad \text{com} \quad q \leq m,$$

logo

$$q^2 \leq q \cdot m = n.$$

Portanto n é divisível por um número primo positivo q tal que $q^2 \leq n$, absurdo. \square

Vamos agora elaborar a tabela (Tabela 1) dos números primos positivos inferiores a 250. Para isso, escrevamos todos os inteiros de 2 a 250. Riscaremos de modo sistemático todos os inteiros compostos que figuram nesta tabela seguindo o roteiro abaixo.

- i) 2 é primo, risque todos os números pares maiores do que 2 pois não são primos;
- ii) Todos os números não riscados inferiores a 4, isto é, o número 3, são primos. Risque todos os múltiplos de 3 maiores do que 3 pois não são primos;
- iii) Todos os números não riscados inferiores a 9, pelo Lema 1, são primos, estes são, 2, 3, 5 e 7. Risque todos os seus múltiplos que ainda não foram riscados;
- iv) Todos os números não riscados inferiores a $7^2 = 49$ são primos, estes são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47. Risque todos os seus múltiplos que ainda não foram riscados;
- v) Como $47^2 > 250$, todos os números não riscados na tabela são primos.

O Crivo de Eratóstenes tem um custo computacional muito elevado tornando-se por isto um método inviável na prática. Até o momento continuamos sem métodos eficazes para elaborar tabelas de números primos. Outras duas questões que ainda não foram resolvidas satisfatoriamente do ponto de vista computacional são a verificação se um dado inteiro é primo (chamada de teste de primalidade) e a

decomposição em fatores primos para inteiros grandes.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230
231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250

Tabela 1 – Os números primos positivos menores do que 250

As duas proposições seguintes caracterizarão certos números primos famosos.

Proposição 1. Sejam a e n inteiros maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.

Demonstração: Suponha que $a^n - 1$ seja primo. Como $a \neq 1$, temos que $(a-1) | (a^n-1)$ (veja Problema 1.8(a), Capítulo 4), logo $a-1 = \pm 1$ ou $a-1 = \pm(a^n-1)$. Segue daí que a única possibilidade é $a = 2$.

Suponha agora que n não seja primo, logo $n = n_1 \cdot n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Como $2^{n_1} - 1$ divide $2^n - 1 = (2^{n_1})^{n_2} - 1$ (veja Problema 1.8 (a), Capítulo 4) e $1 < 2^{n_1} - 1 < 2^n - 1$, segue que $2^n - 1$ não é primo. \square

Os números primos da forma

$$M_p = 2^p - 1,$$

com p primo positivo são chamados de *números de Mersenne* em homenagem a Marin Mersenne (1588-1648) que se interessou pelo problema de determinar números primos p para os quais M_p é um número primo. Mersenne calculou alguns destes primos. No intervalo $2 \leq p \leq 5000$ os números de Mersenne correspondem aos seguintes valores de p : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423.

Proposição 2. *Sejam a e n inteiros maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$ com $m \in \mathbb{Z}^+$.*

Demonstração: Suponha que $a^n + 1$ seja primo. Segue que a tem que ser par pois caso contrário, teríamos que $2 \mid (a^n + 1)$ e $a^n + 1 > 2$, que é absurdo. Escreva agora $n = 2^m \cdot r$ com $m \in \mathbb{Z}^+$, $r \in \mathbb{N}$ e $2 \nmid r$. Queremos provar que $r = 1$. Sendo r ímpar, segue que $a^{2^m} + 1$ divide $a^n + 1 = (a^{2^m})^r + 1$ (veja Problema 1.8(b), Capítulo 4). Como estamos supondo $a^n + 1$ primo, isto só é possível se $a^{2^m} + 1 = a^n + 1$, logo $r = 1$, como queríamos demonstrar. \square

Os números da forma

$$F_m = 2^{2^m} + 1,$$

com $m \in \mathbb{Z}^+$ são chamados de números de Fermat, em homenagem a Pierre de Fermat (1601-1655). Fermat havia conjecturado que F_m era primo para todo $n \geq 0$. Leonhard Euler (1707-1783) mostrou que $F_5 = 2^{32} + 1 = 4.294.967.297$ é divisível por 641 derrubando assim a conjectura de Fermat (veja Problema 1.16, Capítulo 6).

Problemas

1.1 Considere a seguinte função $v: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$, definida por $v(a) =$ número de divisores positivos de a . Mostre que

- (i) Para todo $a \in \mathbb{Z} \setminus \{0\}$, tem-se que $\nu(-a) = \nu(a)$;
- (ii) Se $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ com p_1, \dots, p_n primos distintos e $\alpha_1, \dots, \alpha_n$ inteiros positivos, então $\nu(a) = (\alpha_1 + 1) \cdots (\alpha_n + 1)$;
- (iii) Se $a, b \in \mathbb{Z} \setminus \{0\}$ com $(a, b) = 1$, então $\nu(a \cdot b) = \nu(a) \cdot \nu(b)$.

1.2 Mostre que um inteiro positivo a é um quadrado perfeito se e somente se $\nu(a)$ é ímpar.

1.3 Qual é a expressão geral dos números inteiros que admitem um número primo de divisores positivos?

1.4 Seja p um número primo positivo. Mostre que

- (i) Se $i \in \mathbb{N}$ é tal que $1 \leq i < p$, então $\binom{p}{i}$ é divisível por p ;
- (ii) Se $a, b \in \mathbb{Z}$, então p divide $(a + b)^p - (a^p + b^p)$;
- (iii) Para todo $a \in \mathbb{Z}$ se tem $p \mid (a^p - a)$;
- (iv) Se $a, b \in \mathbb{Z}$, então ou $a^p - b^p$ é primo com p ou $p^2 \mid (a^p - b^p)$.

Sugestão para (iii): Demonstre o resultado por indução sobre a . Este resultado é chamado de *Pequeno Teorema de Fermat*.

1.5 Mostre que para $n \in \mathbb{N}$, não são primos os números

- (i) $2^{4n+2} + 1$
- (ii) $8^n + 1$
- (iii) $2^{4n+2} - 1$
- (iv) $8^{n+1} - 1$

1.6 Sejam a, m e n inteiros tais que $m > n \geq 0$.

- (i) Mostre que $a^{2^n} + 1$ divide $a^{2^m} - 1$;
- (ii) Mostre que

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & , \text{ se } a \text{ é par} \\ 2 & , \text{ se } a \text{ é ímpar} \end{cases}$$

- (iii) Como aplicação de (ii) deduza que $(F_n, F_m) = 1$. Mostre com isto que existem infinitos números primos;

- (iv) Mostre que $2^{2^m} - 1$ tem pelo menos n divisores primos positivos distintos;
- (v) Mostre que se p_n representa o n -ésimo número primo positivo, então

$$p_{n+1} \leq F_n = 2^{2^n} + 1.$$

2. Sobre a Distribuição dos Números Primos

Com os números primos estão relacionados alguns dos problemas mais famosos da Matemática. Alguns destes problemas ainda não foram resolvidos enquanto que outros só foram resolvidos com a utilização de técnicas matemáticas sofisticadas de áreas como a Álgebra, a Análise Real e a Análise Complexa.

Consultando a Tabela 1, note que existem vários pares de números primos que diferem de duas unidades, como por exemplo, (3, 5), (5, 7), (11, 13), (41, 43), (107, 109), (239, 241), entre outros. Pares de primos como estes são chamados de primos gêmeos. Até o presente momento ainda não se sabe se os primos gêmeos são em número finito ou infinito, enquanto que o problema análogo para ternas de primos trigêmeos é de fácil resolução (veja o Problema 2.1).

A distribuição dos números primos é tão irregular que dois primos consecutivos podem ser gêmeos ou, dado um natural n arbitrário, podem diferir por um número maior do que n , como decorre da observação de que não são primos os números,

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n + 1.$$

Por outro lado, um resultado chamado de *Postulado de Bertrand*, conjecturado por Bertrand em 1845 e demonstrado por Chebichev em 1852, afirma que dado um inteiro positivo n , existe sempre um número primo entre n e $2n$. Este é um dos poucos resultados sobre números primos que tem uma demonstração elementar. O leitor interessado neste assunto está convidado a consultar o livro de LeVeque listado na literatura.

Um famoso resultado sobre números primos, diz respeito à função $\pi: \mathbb{N} \rightarrow \mathbb{N}$, definida por $\pi(n) = \text{número de primos positivos menores}$

ou iguais a n . O Teorema de Euclides (Teorema 1) nos diz que

$$\lim_{n \rightarrow \infty} \pi(n) = \infty,$$

e o problema que vinha desafiando os matemáticos, desde o tempo de Gauss, era comparar o crescimento da função π com o crescimento de funções conhecidas. Consultando tabelas de primos pode-se ver que a função π assume valores bastante irregulares e que os números primos são esparsos em \mathbb{N} , isto é, dado um inteiro positivo n , a probabilidade de um número inteiro entre 1 e n ser um número primo, medida pelo número $\pi(n)/n$, se torna pequena à medida que n aumenta. A partir da tabela dos primos menores do que 102.000 publicada por J. Lambert, Gauss determinou empiricamente algo equivalente à seguinte relação:

$$\frac{\pi(n)}{n} \sim \frac{1}{L(n)},$$

onde $L(n)$ significa o logaritmo Neperiano de n e onde o símbolo $f(n) \sim g(n)$ significa que

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1.$$

O primeiro passo na direção da demonstração deste resultado foi dado por Chebichev em 1852, que demonstrou de modo elementar que existem números reais positivos a e b próximos de 1 com $a < 1$ e $b > 1$, tais que

$$\frac{a}{L(n)} < \frac{\pi(n)}{n} < \frac{b}{L(n)}.$$

A relação de Gauss foi demonstrada em 1896 independentemente por J. Hadamard e C. de la Vallée Poussin. A demonstração deste resultado utiliza técnicas de cálculo diferencial e integral e se constitui num importante e difícil teorema de Teoria dos Números, chamado de *Teorema dos Números Primos*.

Outro resultado profundo sobre números primos devido a Dirichlet, provado em 1837 usando técnicas de análise e cuja demonstração está além do nível deste texto, é o seguinte:

Teorema (Dirichlet). *Dados a e r inteiros positivos primos entre si, existe pelo menos um número primo na progressão aritmética de primeiro termo a e razão r.*

Problemas

2.1 Mostre que (3, 5, 7) é a única terna de primos trigêmeos.

Sugestão: Use que $3 | n(n+1)(n+2)(n+3)(n+4)$.

2.2 Assumindo o Postulado de Bertrand mostre que para $n > 1$, o n -ésimo número primo positivo p_n satisfaz a desigualdade $p_n < 2^n$.

2.3 Usando a desigualdade de Chebichev mostre que

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n} = 0.$$

2.4 Usando o teorema dos números primos calcule valores aproximados para $\pi(10^5)$ e para $\pi(10^7)$. Compare os valores obtidos com os seguintes valores exatos: $\pi(10^5) = 9592$ e $\pi(10^7) = 664579$.

2.5 Mostre usando o teorema de Dirichlet que se a e r são inteiros primos entre si, então na progressão aritmética de primeiro termo a e razão r existem infinitos números primos. O que acontece quando a e r não são primos entre si?

2.6 Prove que existem infinitos números primos da forma $4n + 3$.

Sugestão: (i) mostre que todo primo $p \geq 3$ é da forma $4n + 1$ ou $4n + 3$; (ii) mostre que o produto de dois números da forma $4n + 1$ é da mesma forma; (iii) suponha por absurdo que p_k é o último primo positivo da forma $4n + 3$. Considere o número $n = 4(7 \cdot 11 \cdots p_k) + 3$, mostre que ele deveria ser também da forma $4n + 1$ o que é absurdo.

3. Algoritmo de Euclides

Nesta seção apresentaremos o Algoritmo de Euclides que permite calcular efetivamente o máximo divisor comum de dois inteiros. Este método se encontra nos Elementos de Euclides (Livro VII, Proposição

2) e nos permitirá também calcular o mdc de vários inteiros (veja o Problema 3.3).

Recorde que dados inteiros a e b , temos que $\text{mdc}(a, b) = (a, b)$. O seguinte lema nos será útil

Lema 2. *Sejam a, b e m inteiros. Temos então que $(a, 0) = |a|$ e que $(a, b) = (b, a) = (|a|, |b|) = (a - mb, b)$.*

Demonstração: As afirmações seguem das seguintes igualdades que se obtém usando o Lema 2 do Capítulo 4: $I(a, 0) = I(|a|)$ e $I(a, b) = I(b, a) = I(|a|, |b|) = I(a - mb, b)$. \square

Para calcular (a, b) , tendo em vista o lema acima, podemos supor que a e b são não negativos. Se $b = 0$ ou $a = b$, então $(a, b) = a$, nada tendo que calcular. Suponhamos que $a \neq b$, como $(a, b) = (b, a)$, podemos finalmente supor que $a > b > 0$.

Pela divisão euclidiana temos que

$$a = b \cdot q_1 + r_2 , \quad 0 \leq r_2 < b.$$

Da igualdade acima e do Lema 2 segue que

$$(a, b) = (a - b \cdot q_1, b) = (r_2, b) = (b, r_2).$$

Dois casos podem se apresentar:

- 1) $r_2 = 0$. Neste caso, temos $(a, b) = (b, r_2) = (b, 0) = b$;
- 2) $r_2 \neq 0$. Neste caso efetuamos a divisão euclidiana de b por r_2 , obtendo

$$b = r_2 \cdot q_2 + r_3 , \quad 0 \leq r_3 < r_2.$$

Argumentando como acima segue que $(a, b) = (b, r_2) = (r_2, r_3)$.

Novamente dois casos podem se apresentar

- 1') $r_3 = 0$. Neste caso, $(a, b) = (r_2, 0) = r_2$;
- 2') $r_3 \neq 0$. Neste caso efetuamos a divisão euclidiana r_2 por r_3 , obtendo

$$r_2 = r_3 \cdot q_3 + r_4 , \quad 0 \leq r_4 < r_3.$$

Novamente procedendo como acima temos que

$$(a, b) = (b, r_2) = (r_2, r_3) = (r_3, r_4),$$

e assim sucessivamente.

Definindo $r_1 = b$, segue da argumentação acima que existe um valor de n tal que $r_{n+1} = 0$ e $r_n \neq 0$. De fato, se para todo n , tivessemos $r_n \neq 0$, teríamos uma seqüência infinita r_1, r_2, r_3, \dots tal que

$$r_1 > r_2 > r_3 > \dots > 0,$$

contrariando o Princípio da Boa Ordenação.

Segue então que

$$(a, b) = (b, r_2) = \dots = (r_n, r_{n+1}) = (r_n, 0) = r_n,$$

portanto o último resto não nulo r_n neste processo nos fornece o valor de (a, b) .

Note que o procedimento acima é uma outra demonstração, desta vez construtiva, da existência de mdc em \mathbb{Z} .

Calcularemos efetivamente o número (a, b) com a ajuda do seguinte dispositivo prático que decorre imediatamente do procedimento acima que chamamos de *Algoritmo de Euclides*:

	q_1	q_2	q_3	\dots	q_{n-2}	q_{n-1}	q_n
a	b	r_2	r_3	\dots	r_{n-2}	r_{n-1}	r_n
r_2	r_3	r_4	r_5	\dots	r_n	0	

Exemplos

1. Calculemos $(330, 240)$.

	1	2	1	2
330	240	90	60	30
90	60	30	0	

$$(330, 240) = 30.$$

2. Calculemos $(484, 1521)$.

	3	7	69
1521	484	69	1
69	1	0	

$$(484, 1521) = 1.$$

Como em particular $(a, b) \in I(a, b)$, existem inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$. O algoritmo de Euclides usado de trás para frente permite calcular tais inteiros. De fato, considere as seguintes igualdades:

$$\begin{aligned} (1) \quad r_n &= r_{n-2} - q_{n-1} \cdot r_{n-1}; \\ (2) \quad r_{n-1} &= r_{n-3} - q_{n-2} \cdot r_{n-2}; \\ (3) \quad r_{n-2} &= r_{n-4} - q_{n-3} \cdot r_{n-3}; \\ \vdots &\qquad \vdots \\ (n-2) \quad r_3 &= b - q_2 \cdot r_2; \\ (n-1) \quad r_2 &= a - q_1 \cdot b. \end{aligned}$$

Substituindo o valor de r_{n-1} de (2) em (1), obtemos

$$r_n = (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-2} - q_{n-1} \cdot r_{n-3},$$

substituindo nesta igualdade o valor de r_{n-2} de (3), obtemos

$$r_n = -(q_{n-3} + q_{n-1} \cdot q_{n-2} \cdot q_{n-3} + q_{n-1}) \cdot r_{n-3} + (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-4}.$$

Assim sucessivamente até obter no final os inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$.

Exemplos

3. No exemplo 1 acima, temos

$$\begin{aligned} 30 &= 90 - 1 \cdot 60 \\ 60 &= 240 - 2 \cdot 90 \\ 90 &= 330 - 1 \cdot 240. \end{aligned}$$

Substituindo como acenamos acima, temos:

$$\begin{aligned} 30 &= 90 - 1 \cdot (240 - 2 \cdot 90) = 3 \cdot 90 - 240 \\ &= 3 \cdot (330 - 240) - 240 = 3 \cdot 330 - 4 \cdot 240. \end{aligned}$$

Logo $m_0 = 3$ e $n_0 = -4$.

4. No exemplo 2 acima, temos

$$\begin{aligned} 1 &= 484 - 7 \cdot 69 \\ 69 &= 1521 - 3 \cdot 484. \end{aligned}$$

Fazendo substituições sucessivas, temos:

$$1 = 484 - 7 \cdot 69 = 484 - 7 \cdot (1521 - 3 \cdot 484) = 22 \cdot 484 - 7 \cdot 1521.$$

Logo, $m_0 = 22$ e $n_0 = -7$.

O algoritmo de Euclides é um dos primeiros exemplos na história da Matemática de método de cálculo recursivo. Este método por ser um importante método de cálculo em computação, ganhou nos nossos dias maior destaque. O leitor a título de exercício poderá escrever um programa na linguagem de sua preferência para calcular o número (a, b) e os inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$.

Uma questão muito importante para os interessados nos aspectos computacionais é a eficiência ou o custo de um dado algoritmo. Vejamos agora qual é o custo do algoritmo de Euclides.

Na demonstração do próximo teorema utilizaremos o fato da função logaritmo na base 2 ser monótona crescente e a seguinte desigualdade simples de verificar. Para todo $m \in \mathbb{N}$,

$$\left[\frac{m}{2} \right] \geq \frac{m}{2} - \frac{1}{2}.$$

Teorema 2. *O número de iterações no algoritmo de Euclides para calcular o mdc de dois inteiros positivos a e b com $a > b$, é inferior a $2(1 + \log_2 b)$.*

Demonstração: O algoritmo de Euclides se escreve

$$\begin{aligned} a &= bq_1 + r_2 \quad , \quad 0 \leq r_2 < b \\ b &= r_2 q_2 + r_3 \quad , \quad 0 \leq r_3 < r_2 \\ r_2 &= r_3 q_3 + r_4 \quad , \quad 0 \leq r_4 < r_3 \\ &\vdots \\ r_{n-1} &= r_n q_n + r_{n+1} \quad , \quad r_{n+1} = 0. \end{aligned}$$

Pela Observação 2 após o Teorema 6, Capítulo 3, temos, para $i = 1, 2, \dots, n - 1$, que

$$r_{i+2} < \frac{r_i}{2},$$

onde colocamos $r_1 = b$. Logo

$$1 \leq r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{2^2} < \dots < \frac{r_{n-2}[\frac{n-1}{2}]}{2^{[\frac{n-1}{2}]}} \leq \frac{b}{2^{[\frac{n-1}{2}]}}$$

portanto

$$2^{[\frac{n-1}{2}]} < b,$$

e consequentemente,

$$\left[\frac{n-1}{2} \right] < \log_2 b.$$

Como $\left[\frac{n-1}{2} \right] \geq \frac{n-1}{2} - \frac{1}{2}$, segue que

$$n < 2(1 + \log_2 b)$$

Como n é o número de iterações para calcular o mdc, o resultado segue. \square

Com um pouco mais de trabalho, é possível mostrar que o número de iterações é de fato não superior a $5 \log_{10} b$.

Um resultado curioso relacionado com a noção de mdc é o seguinte teorema de Cesaro demonstrado em 1881 e que apenas enunciamos

Teorema (Cesaro). Se a e b são inteiros positivos escolhidos ao acaso, então a probabilidade de que $(a, b) = 1$ é $6/\pi^2$ (aproximadamente 61%).

Problemas

3.1 Para cada par de inteiros a e b dados abaixo ache os inteiros (m, n) e $\text{mmc}(a, b)$ além de inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$.

- | | |
|------------------|-----------------|
| (i) 637, 3887 | (ii) 648, -1218 |
| (iii) -551, -874 | (iv) 7325, 8485 |

3.2 Dado um inteiro n , maior do que 1 em (iii), mostre que

- | | |
|------------------------------------|-----------------------------|
| (i) $(n, 2n + 1) = 1$ | (ii) $(2n + 1, 3n + 1) = 1$ |
| (iii) $(n! + 1, (n + 1)! + 1) = 1$ | |

3.3 Calcule $(325, 275, 450)$

Sugestão: Use o resultado do Problema 2.6 (b), Capítulo 4 e o Algoritmo de Euclides.

3.4 Sejam $a \in \mathbb{Z} \setminus \{-1, 1\}$ e $m, n \in \mathbb{N}$ e seja $d = (m, n)$. Mostre que

$$(a^m - 1, a^n - 1) = a^d - 1.$$

4. Equações Diofantinas

Diofanto viveu presumivelmente no século III em Alexandria, já sob o domínio de Roma. Foi praticamente o único matemático de renome na Grécia antiga que se dedicou predominantemente à teoria dos números. Interessou-se por uma grande variedade de equações para as quais procurava soluções racionais e eventualmente inteiiras.

O tratamento algébrico dado por Diofanto à teoria dos números difere do de seus predecessores que utilizavam métodos geométricos para deduzir as suas asserções.

Hoje chamam-se de *Equações Diofantinas* às equações polinomiais com coeficientes inteiros (para as quais só se está interessado em soluções inteiiras ou racionais).

As equações Diofantinas das quais nos ocuparemos aqui são de um tipo muito especial, a saber, são da forma

$$ax + by = n,$$

com a, b e n inteiros.

Dada uma tal equação, é natural formular as seguintes perguntas:

- Sob quais condições a equação admite soluções?
- Quando existem soluções, como determiná-las?

Os próximos dois teoremas nos darão respostas a estas perguntas.

Teorema 3. *A equação $ax + by = n$ admite solução se, e somente se, $(a, b) \mid n$.*

Demonstração: Suponha que a equação admita uma solução x_0, y_0 , isto é, $a \cdot x_0 + b \cdot y_0 = n$. Como (a, b) divide a e divide b , segue que divide $a \cdot x_0 + b \cdot y_0 = n$.

Reciprocamente, suponha que $(a, b) \mid n$. Então existe um inteiro t tal que $n = t \cdot (a, b)$. Como existem inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$, segue que $n = t \cdot (a, b) = (t \cdot m_0) \cdot a + (t \cdot n_0) \cdot b$. Logo os inteiros $x_0 = t \cdot m_0$ e $y_0 = t \cdot n_0$ são uma solução da equação.

□

Teorema 4. *Seja x_0, y_0 uma solução particular da equação $ax + by = n$. Tem-se que x, y é uma solução da equação se, e somente se,*

$$x = x_0 + t \cdot \frac{b}{(a, b)} \quad \text{e} \quad y = y_0 - t \cdot \frac{a}{(a, b)},$$

para algum t em \mathbb{Z} .

Demonstração: Substituindo x e y da forma acima, na equação, vê-se facilmente que se trata de uma solução.

Reciprocamente, se $a = 0$ ou $b = 0$, é claro que toda solução é da forma acima.

Suponha que $a \cdot b \neq 0$ e x, y é uma solução, então

$$n = a \cdot x + b \cdot y = a \cdot x_0 + b \cdot y_0.$$

Segue daí que

$$a \cdot (x - x_0) = b \cdot (y_0 - y), \tag{1}$$

portanto,

$$\frac{a}{(a, b)} \cdot (x - x_0) = \frac{b}{(a, b)} \cdot (y_0 - y).$$

Como $(a/(a, b), b/(a, b)) = 1$ (veja Problema 3.4, Capítulo 4), segue que $(a/(a, b)) \mid (y_0 - y)$ e $(b/(a, b)) \mid (x - x_0)$. Portanto existem inteiros m e t tais que $y_0 - y = t \cdot (a/(a, b))$ e $x - x_0 = m \cdot (b/(a, b))$. Substituindo estes valores em (1), obtém-se $m = t$, logo

$$x = x_0 + t \cdot \frac{b}{(a, b)} \quad \text{e} \quad y = y_0 - t \cdot \frac{a}{(a, b)}. \quad \square$$

Segue do teorema que se a equação admite uma solução, ela admitirá uma infinidade de soluções. Qualquer uma destas soluções determina todas as outras.

Para determinar uma solução particular da equação, quando a e b são números pequenos, procede-se por inspeção. Se não for possível por este método achar uma solução, o método seguinte é efetivo.

Ache com o algoritmo de Euclides inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$. Multiplique ambos os lados desta igualdade por $n/(a, b)$, obtendo $(n/(a, b)) \cdot m_0 \cdot a + (n/(a, b)) \cdot n_0 \cdot b = n$. Portanto $x_0 = (n/(a, b)) \cdot m_0$ e $y_0 = (n/(a, b)) \cdot n_0$, é uma solução particular da equação.

Exemplos

1. A equação $9x + 12y = 1$ não admite solução pois $(9, 12) = 3$ e $3 \nmid 1$.
2. Resolvamos a equação $28x + 90y = 22$. Inicialmente temos que calcular $(28, 90)$.

	3	4	1	2
90	28	6	4	2
6	4	2	0	

Visto que $(28, 90) = 2$ e $2 \mid 22$, a equação admite soluções. Usando o

algoritmo de trás para frente, temos

$$\begin{aligned} 2 &= 6 - 1 \cdot 4 \\ 4 &= 28 - 4 \cdot 6 \\ 6 &= 90 - 3 \cdot 28 \end{aligned}$$

Segue que

$$\begin{aligned} 2 &= 6 - 1 \cdot (28 - 4 \cdot 6) = (-1) \cdot 28 + 5 \cdot 6 \\ &= (-1) \cdot 28 + 5 \cdot (90 - 3 \cdot 28) \\ &= (-16) \cdot 28 + 5 \cdot 90. \end{aligned}$$

Logo $2 = (-16) \cdot 28 + 5 \cdot 90$.

Multiplicando ambos os membros desta igualdade por 11, temos

$$22 = (-176) \cdot 28 + 55 \cdot 99.$$

Portanto, uma solução particular da equação é dada por $(x_0, y_0) = (-176, 55)$. Pelo Teorema 4, a solução geral é

$$x = -176 + t \cdot 45 \quad \text{e} \quad y = 55 - t \cdot 14, \quad t \in \mathbb{Z}.$$

A equação $ax + by = n$ foi resolvida pelo matemático hindu do século VII, Brahmagupta.

Muitas outras equações Diofantinas foram estudadas. Algumas, como por exemplo as que consideramos, resolvem-se utilizando métodos elementares, outras requerem métodos mais sofisticados. Uma equação estudada desde a antiguidade, é a *equação pitagórica*:

$$x^2 + y^2 = z^2.$$

Esta equação que será estudada no Capítulo 10, possui infinitas soluções e existem fórmulas que permitem gerar todas elas. Pierre de Fermat afirmou sem dar uma demonstração que a equação

$$x^n + y^n = z^n,$$

para $n > 2$, não admitia soluções em inteiros positivos. A esta afirmação chama-se de o *Último Teorema de Fermat*.

Observe também que os Teoremas 3 e 4 são válidos no contexto mais geral dos domínios principais.

Problemas

4.1 Resolva as equações:

- | | | |
|---------------------|-----------------------|------------------------|
| a) $7x - 9y = 1$ | b) $4x - 3y = 2$ | c) $6x + 4y = 3$ |
| d) $6x + 4y = 6$ | e) $12x - 18y = 360$ | f) $144x + 125y = 329$ |
| g) $36x - 21y = 31$ | h) $350x - 91y = 731$ | |

4.2 Dada a equação $ax + by = n$ com a e b positivos, mostre que o número de soluções positivas desta equação é no máximo finito.

4.3 Sejam $a, b, c, d, n, m \in \mathbb{Z}$ com $D = a \cdot d - b \cdot c \neq 0$. Mostre que o sistema de equações simultâneas

$$\begin{cases} ax + by = n \\ cx + dy = m \end{cases}$$

admite solução se, e somente se, D divide $n \cdot d - m \cdot b$ e $m \cdot a - n \cdot c$. Neste caso, o sistema admite uma única solução. Determine esta solução.

4.4 Mostre que a equação $a_1x_1 + \dots + a_nx_n = b$ com $a_1, \dots, a_n, b \in \mathbb{Z}$, admite solução em inteiros se, e somente se, $(a_1, \dots, a_n) | b$.

5. O Despertar da Aritmética

Após os trabalhos de Diofanto seguiram-se muitos séculos sem que a Aritmética registrasse um grande salto qualitativo do ponto de vista teórico. Houve neste ínterim a criação do sistema de numeração decimal posicional e a introdução do zero pelos hindus, a sua adoção pelos árabes e a sua utilização ainda que tardia na Europa. Durante este longo período foram aperfeiçoados os algoritmos para efetuar as operações, as frações e a Aritmética Financeira.

A Aritmética Teórica teve o seu despertar no século 17 por obra do jurista francês e matemático amador Pierre de Fermat (1601-1665). Fermat enunciou vários teoremas dos quais raramente dava as demonstrações. Muitas delas foram dadas posteriormente por outros matemáticos ficando porém em aberto até recentemente o já citado Último Teorema de Fermat.

Nas suas leituras de uma tradução da Aritmética de Diofanto, Fermat anotava as suas observações nas margens do livro. No seu comentário ao oitavo problema do segundo livro que trata da resolução da equação pitagórica $x^2 + y^2 = z^2$, Fermat escreveu:

“Ao contrário, é impossível separar um cubo em dois cubos, uma potência quarta em duas potências quartas, ou em geral, qualquer potência acima da segunda em duas potências do mesmo grau. Eu descobri uma demonstração verdadeiramente maravilhosa que esta margem é muito estreita para conter”.

Quase três séculos e meio se passaram até que se tenha conseguido provar esta afirmação. Foram produzidas ao longo do tempo provas da veracidade da asserção para vários valores de n e inúmeras vezes foram enunciadas falsas demonstrações do teorema.

Finalmente, em 1993 Andrew Wiles anunciou que havia demonstrado o Último Teorema de Fermat exibindo um manuscrito de cerca de 200 páginas contendo o que afirmava ser a demonstração do teorema. Foram necessários dois anos para que os especialistas analisassesem este trabalho e que o próprio Wiles esclarecesse vários pontos para que a prova fosse reconhecida como correta e completa. Foi assim vencido um dos maiores desafios da Matemática, sendo difícil acreditar que Fermat tivesse realmente a demonstração deste teorema.

Grande parte dos teoremas enunciados por Fermat foram posteriormente provados pelo matemático suíço Leonhard Euler (1707-1783). Euler teve uma produção científica fabulosa, tendo sido o matemático mais produtivo de todos os tempos. Estima-se que ao longo de 55 anos de atividades ele tenha escrito trabalhos que não caberiam em 80 grossos volumes. Esta produtividade sequer baixou nos últimos 17 anos de sua vida passados em estado de cegueira total.

Grandes matemáticos como Legendre, Gauss, Dirichlet, Dedekind, Riemann e Hilbert, só para citar alguns, contribuiram para o desenvolvimento posterior da Teoria dos Números, considerada por muitos a área mais nobre da Matemática.

Congruências

As congruências são o instrumento adequado quando se quer dar ênfase ao resto na divisão euclidiana. Elas foram introduzidas e extensivamente estudadas por Gauss no seu famoso “*Disquisitiones Arithmeticae*”, publicado em 1801. As noções introduzidas por Gauss e suas notações foram imediatamente adotadas pelos matemáticos da época e são ainda usadas atualmente. Este capítulo destina-se a introduzir a noção de congruência, apresentar as suas propriedades básicas e oferecer algumas aplicações.

1. Propriedades das Congruências

Seja m um inteiro não nulo. Dois inteiros a e b serão ditos *congruentes módulo m* se os restos de a e b por m forem iguais. Quando a e b são congruentes módulo m , escrevemos $a \equiv b \pmod{m}$.

Exemplos. $12 \equiv 17 \pmod{5}$, $15 \equiv 0 \pmod{3}$, $15 \equiv -1 \pmod{4}$.

Note que $a \equiv b \pmod{m}$ se e somente se $a \equiv b \pmod{-m}$ pois de $a = m \cdot q + r$ e $b = m \cdot q' + r$ com $0 \leq r < |m|$, decorre que $a = (-m)(-q) + r$ e $b = (-m)(-q') + r$ com $0 \leq r < |-m|$ e vice-versa. Portanto, no que diz respeito aos restos, basta considerarmos congruências módulos inteiros positivos.

Como $a \equiv b \pmod{1}$, quaisquer que sejam os inteiros a e b , é portanto sem interesse a noção de congruência neste caso. No que se segue vamos sempre supor $m > 1$.

Dois números não congruentes módulo m serão ditos *incongruentes módulo m*.

Uma maneira mais simples de verificar se dois números são congruentes é dada pela seguinte proposição.

Proposição 1. *Tem-se que $a \equiv b \pmod{m}$ se e somente se $m | (a - b)$.*

Demonstração: Se $a \equiv b \pmod{m}$, então existem inteiros r, q e q' tais que $a = m \cdot q + r$ e $b = m \cdot q' + r$, logo $a - b = m(q - q')$ e consequentemente $m | (a - b)$.

Reciprocamente, suponha que $m | (a - b)$. Pela divisão euclidiana, temos que $a = m \cdot q + r$ e $b = m \cdot q' + r'$ com $0 \leq r < m$ e $0 \leq r' < m$, logo $a - b = m(q - q') + r - r'$. Como $m | m(q - q')$, segue que $m | (r - r')$, logo $r = r'$ pois $|r - r'| < m$. Portanto $a \equiv b \pmod{m}$.

□

Proposição 2. *Sejam a, b, c, d, m e n inteiros com $m > 1$ e $n \geq 1$. Temos que*

- (i) $a \equiv a \pmod{m}$;
- (ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;
- (iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$;
- (iv) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$;
- (v) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \cdot c \equiv b \cdot d \pmod{m}$;
- (vi) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.

Demonstração: i. e ii. são imediatas.

iii. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$, logo $m | (a - b + b - c)$, donde $m | (a - c)$ e portanto $a \equiv c \pmod{m}$.

iv. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, segue que $m | (a - b)$ e $m | (c - d)$, logo $m | (a - b + c - d)$ e portanto $a + c \equiv b + d \pmod{m}$.

v. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, segue que $m | (a - b)$ e $m | (c - d)$. Como

$$ac - bd = a(c - d) + d(a - b),$$

segue que $m | (ac - bd)$ e consequentemente $ac \equiv bd \pmod{m}$.

vi. Isto segue de (v), por indução sobre n .

□

As propriedades (i), (ii) e (iii) na proposição acima nos dizem que a relação de congruência módulo m em \mathbb{Z} é uma relação de equivalência, enquanto que as propriedades (iv) e (v) são de compatibilidade da relação com as operações de adição e multiplicação.

Vejamos agora alguns exemplos que nos revelarão a riqueza do campo de aplicações da noção de congruência.

Exemplos

1. Para achar o resto da divisão de a por m basta achar um inteiro r tal que $a \equiv r \pmod{m}$ e $0 \leq r < m$. Para acharmos o resto da divisão de 2^{30} por 17 sem usar nenhum resultado especial, deveríamos calcular inicialmente o valor de 2^{30} para posteriormente dividí-lo por 17, o que representaria um trabalho considerável. Vejamos como a noção de congruência torna mais suave esta tarefa.

Note que $2^4 \equiv -1 \pmod{17}$, elevando ambos os membros à potência 7 temos pela Proposição 2, (vi), que $2^{28} \equiv -1 \pmod{17}$. Multiplicando ambos os membros desta igualdade por 4, pela Proposição 2 (v), segue que $2^{30} \equiv -4 \pmod{17}$. Como $-4 \equiv 13 \pmod{17}$, segue pela Proposição 2 (iii), que $2^{30} \equiv 13 \pmod{17}$. Concluímos com isto que o resto da divisão de 2^{30} por 17 é 13.

2. Neste exemplo estabeleceremos critérios de divisibilidade por 2, 5 e 10.

Observe que $10 \equiv 0 \pmod{2}$, $10 \equiv 0 \pmod{5}$ e $10 \equiv 0 \pmod{10}$, consequentemente para todo $i \in \mathbb{N}$ temos que $10^i \equiv 0 \pmod{2}$, $\pmod{5}$ e $\pmod{10}$. Se $a = a_n a_{n-1} \cdots a_2 a_1 a_0$ é um inteiro representado na base 10, temos que $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$, logo $a \equiv a_0 \pmod{2}$, $\pmod{5}$ e $\pmod{10}$. Portanto a é divisível por 10, por 5 ou por 2 se e somente se $a_0 \equiv 0 \pmod{10}$, $\pmod{5}$ ou $\pmod{2}$, respectivamente. Deduzimos daí os seguintes critérios para números representados na base 10.

- (a) Um número é divisível por 10 se e somente se o seu algarismo da unidade é zero;
- (b) Um número é divisível por 5 se e somente se o seu algarismo da unidade é zero ou 5;

- (c) Um número é divisível por 2 se e somente se o seu algarismo da unidade é par.

3. Estabelecemos neste exemplo critérios de divisibilidade por 9 e por 3. De $10 \equiv 1 \pmod{9}$ ou $\pmod{3}$, segue pela Proposição 2 (vi), que $10^i \equiv 1 \pmod{9}$ ou $\pmod{3}$ para todo $i \in \mathbb{Z}^+$. Seja $a = a_n a_{n-1} \cdots a_1 a_0$ um inteiro positivo representado na base 10, temos então que

$$a \equiv a_0 + a_1 + \cdots + a_n \pmod{9}, \pmod{3}.$$

Deduzimos daí os seguintes critérios:

Um inteiro é divisível por 9 (respectivamente por 3) se e somente se a soma dos algarismos de sua representação na base 10 for divisível por 9 (respectivamente por 3).

Na soma $a_0 + a_1 + \cdots + a_n$ cada parte igual a nove se elimina pois é congruente a zero módulo 9. Isto é a regra dos “noves fora”.

4. Neste exemplo discutimos a “*prova dos nove*”.

A “*prova dos nove*” é um teste para detectar erros nas quatro operações. A título de exemplo, vejamos como ela funciona no caso da multiplicação.

Sejam

$$a = a_n a_{n-1} \cdots a_1 a_0,$$

$$b = b_m b_{m-1} \cdots b_1 b_0, \quad \text{e}$$

$$c = c_r c_{r-1} \cdots c_1 c_0,$$

três inteiros representados na base 10 e suponha que se tenha efetuado a operação $a \cdot b = c$. Seja a' o valor de $a_0 + a_1 + \cdots + a_n$ após ter posto os noves fora, analogamente para b' e c' . Seja d' o valor de $a' \cdot b'$ após ter posto os noves fora, devemos então ter $c' = d'$. Usa-se na prática o seguinte diagrama:

$$\begin{array}{ccc} & a' & \\ d' & \cdot & c' \\ & b' & \end{array}$$

Se $d' \neq c'$, então certamente houve um erro na conta. Caso

$d' = c'$ não podemos concluir que a conta esteja correta, mas com certeza ela se torna mais confiável por ter passado por um teste.

5. Critério de divisibilidade por 11.

Note que $10 \equiv -1 \pmod{11}$, logo

$$10^i \equiv \begin{cases} 1 \pmod{11} & , \text{ se } i \text{ é par} \\ -1 \pmod{11} & , \text{ se } i \text{ é ímpar} \end{cases}$$

Seja $a = a_n a_{n-1} \cdots a_1 a_0$ um número inteiro representado na base 10. Temos que

$$a = a_0 + a_1 \cdot 10 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n,$$

logo

$$a \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \pmod{11}.$$

Deduzimos daí o seguinte critério:

Um inteiro é divisível por 11 se, e somente se, a diferença entre a soma dos algarismos de ordem par e a soma dos algarismos de ordem ímpar da sua representação decimal for divisível por 11.

Vejamos agora algumas propriedades das congruências relacionadas com a divisão.

Proposição 3. Sejam $a, b, c, m, n \in \mathbb{Z}$ com $m > 1$ e $n > 1$.

- (i) Se $a \equiv b \pmod{m}$ e $n | m$, então $a \equiv b \pmod{n}$;
- (ii) $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$ se e somente se
 $a \equiv b \pmod{\text{mmc}(m, n)}$;
- (iii) Se $a \cdot c \equiv b \cdot c \pmod{m}$ e $(c, m) = 1$, então $a \equiv b \pmod{m}$;
- (iv) Se $d = (c, m)$, então $a \cdot c \equiv b \cdot c \pmod{m}$ se e somente se
 $a \equiv b \pmod{\frac{m}{d}}$.

Demonstração: i. Se $a \equiv b \pmod{m}$, então $m | (a - b)$ e como $n | m$, segue que $n | (a - b)$, logo $a \equiv b \pmod{n}$.

ii. Se $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$, temos que $m | (a - b)$ e $n | (a - b)$, logo pela definição de mmc temos que $\text{mmc}(m, n) | (a - b)$ e portanto $a \equiv b \pmod{\text{mmc}(m, n)}$.

Reciprocamente, se $a \equiv b \pmod{\text{mmc}(m, n)}$, temos de (i) que $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$ pois $m \mid \text{mmc}(m, n)$ e $n \mid \text{mmc}(m, n)$.

iii. Se $a \cdot c \equiv b \cdot c \pmod{m}$, então $m \mid [c \cdot (a - b)]$ e como $(c, m) = 1$, segue que $m \mid (a - b)$ e portanto $a \equiv b \pmod{m}$.

iv. Se $a \cdot c \equiv b \cdot c \pmod{m}$, segue que $m \mid [c \cdot (a - b)]$, donde $c \cdot (a - b) = t \cdot m$ para algum $t \in \mathbb{Z}$. Sendo $d = (c, m)$, temos que

$$\frac{c}{d} \cdot (a - b) = t \cdot \frac{m}{d}$$

com

$$\left(\frac{c}{d}, \frac{m}{d}\right) = 1$$

(veja Problema 3.4, Capítulo 3). Como

$$\frac{c}{d} \cdot a \equiv \frac{c}{d} \cdot b \pmod{\frac{m}{d}},$$

segue, de (iii) acima, que $a \equiv b \pmod{\frac{m}{d}}$.

Reciprocamente, sejam $c_0, m_0 \in \mathbb{Z}$ tais que $c = c_0 \cdot d$ e $m = m_0 \cdot d$. Por hipótese $a \equiv b \pmod{m_0}$, logo $a - b = t \cdot m_0$ para algum $t \in \mathbb{Z}$, portanto $c \cdot (a - b) = t \cdot m_0 \cdot c = t \cdot m_0 \cdot c_0 \cdot d = t \cdot c_0 \cdot m$ e consequentemente, $ac \equiv bc \pmod{m}$. \square

Corolário. Sejam $a, b, m, m_1, \dots, m_r \in \mathbb{Z}$ com $m, m_1, \dots, m_r > 1$. Suponha que $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ seja a decomposição de m em fatores primos distintos. Temos que

- (i) Se $a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_r}$, então $a \equiv b \pmod{\text{mmc}(m_1, \dots, m_r)}$;
- (ii) $a \equiv b \pmod{m}$ se e somente se $a \equiv b \pmod{p_1^{\alpha_1}}, \dots,$
 $a \equiv b \pmod{p_s^{\alpha_s}}$;
- (iii) Se $a \equiv b \pmod{p_i^{\alpha_i}}$, então $a \equiv b \pmod{p_i}$.

Demonstração: As demonstrações são imediatas e serão omitidas. \square

Problemas

1.1 Verifique a veracidade ou falsidade das seguintes afirmações

- (a) $7 \equiv 24 \pmod{5}$
 (c) $529 \equiv -8 \pmod{3}$

- (b) $33 \equiv 57 \pmod{6}$
 (d) $-12 \equiv -72 \pmod{8}$

1.2 Ache a solução geral e a menor solução positiva de cada congruência abaixo:

- (a) $x \equiv 7 \pmod{3}$
 (c) $3x + 2 \equiv 0 \pmod{7}$

- (b) $x \equiv -1 \pmod{6}$
 (d) $14x + 3 \equiv 0 \pmod{21}$

1.3 Seja $n \in \mathbb{Z}^+$, mostre que

- (a) $19^{8n} - 1$ é divisível por 17 para todo n ;
 (b) $13^{3n} + 17^{3n}$ é divisível por 45 para todo n ímpar.

1.4 Mostre que se $n \in \mathbb{Z}^+$, o algarismo das unidades na representação na base 10 de 3^n só pode ser 1, 3, 7 ou 9. Ache os algarismos das unidades de $3^{400}, 3^{401}, 3^{402}$ e 3^{403} .

1.5 Ache, na base 10, critérios de divisibilidade por

- (a) 4, 25 e 100;
 (b) 8, 125 e 1000;
 (c) generalize.

1.6 Determine os algarismos x, y e z em cada caso para que os números abaixo, representados na base 10, tenham a propriedade mencionada

- (a) $2x7y$ é divisível por 11 e por 4;
 (b) $28x75y$ é divisível por 3 e por 11;
 (c) $45xy$ é divisível por 4 e por 9;
 (d) $13xy45z$ é divisível por 8, por 9 e por 11.

1.7 Mostre que, para que um número seja divisível por 6 é necessário e suficiente que na sua representação na base 10, a soma do algarismo da unidade com quatro vezes cada um dos outros algarismos, seja divisível por 6.

1.8 Da igualdade $1001 = 7 \times 11 \times 13$, deduza os seguintes critérios de divisibilidade por 7, por 11 e por 13:

Dado $a = a_n a_{n-1} \cdots a_1 a_0$, escrito na base 10, então a é divisível por 7, por 11 ou por 13 se e somente se $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$ é divisível por 7 por 11 ou por 13 respectivamente.

1.9 Mostre que dado um número qualquer representado na base 10,

- (a) se subtrairmos do número a soma dos seus algarismos, o resultado é divisível por 9;
- (b) se subtrairmos do número outro qualquer formado por uma permutação dos seus algarismos, o resultado é divisível por 9.

1.10 (O Pequeno Teorema de Fermat). Seja p um número primo positivo, mostre que

- (a) Se a é um inteiro qualquer, então $a^p \equiv a \pmod{p}$;
- (b) Se a é um inteiro não divisível por p , então $a^{p-1} \equiv 1 \pmod{p}$.

Sugestão: (Para (a)) Por indução sobre a ou senão veja Problema 1.4, Capítulo 5

1.11 Ache o resto da divisão

- (a) de 11^{p-1} por p , se p é primo;
- (b) de 2^{100} por 11.

Sugestão: Use o Pequeno Teorema de Fermat.

1.12 Ache o menor inteiro positivo que deixa restos 5, 4, 3 e 2 quando dividido respectivamente por 6, 5, 4 e 3.

Sugestão: Note que $5 \equiv -1 \pmod{6}$, $4 \equiv -1 \pmod{5}$, etc. Use então o item (ii) da Proposição 3.

1.13 Ache o menor múltiplo positivo de 7 que tem resto 1 quando dividido por 2, 3, 4, 5 e 6.

1.14 Ache o menor inteiro positivo que deixa restos 9, 8, 7, ..., 1 quando dividido respectivamente por 10, 9, 8, ..., 2.

1.15 Mostre que

- (a) se p é um número primo ímpar positivo tal que $p \mid (a^{2^r} + 1)$ para algum $a > 1$, então $p \equiv 1 \pmod{2^{r+1}}$;

Sugestão: Por indução sobre r e redução ao absurdo utilizando o Pequeno Teorema de Fermat.

- (b) todo divisor primo positivo p de um número de Fermat $F_n = 2^{2^n} + 1$ é da forma $p = 1 + x \cdot 2^{n+1}$ para algum $x \in \mathbb{N}$. Ache os cinco menores primos positivos que podem dividir F_5 e teste-os. Conclua com Euler que F_5 não é primo contrariamente ao que Fermat havia afirmado;
- (c) para cada $r \in \mathbb{N}$, existem infinitos primos da forma $1 + n \cdot 2^r$. Isto é um caso particular do Teorema de Dirichlet (Capítulo 5, Seção 2). Em particular existem infinitos números primos da forma $4n + 1$.

Sugestão: Use o Problema 1.6, (iii), Capítulo 5, para mostrar que é infinito, para cada $r \in \mathbb{N}$, o conjunto

$$\Lambda_r = \{p > 0 \mid p \text{ é divisor primo de } F_n \text{ para algum } n > r - 1\}$$

1.16 Seja p um número primo positivo e sejam

$$m = m_0 + m_1p + \cdots + m_sp^s$$

e

$$n = n_0 + n_1p + \cdots + n_sp^s$$

com $m_i, n_i \in \mathbb{Z}^+$ para $i = 0, \dots, s$.

- (a) Mostre que $(pm)! = p^m \cdot m!M$, com M inteiro tal que $M \equiv [(p-1)!]^m \pmod{p}$;
- (b) Mostre que $\binom{pm}{pn} \equiv \binom{m}{n} \pmod{p}$;
- (c) Mostre que $\binom{m}{n} \equiv \binom{m-m_0}{n-n_0} \binom{m_0}{n_0} \pmod{p}$;
- (d) Mostre que $\binom{m}{n} \equiv \binom{m_0}{n_0} \cdots \binom{m_s}{n_s} \pmod{p}$.

Sugestão: (Para (a)) Escreva

$$(pm)! = p \cdot 2p \cdots mp[1 \cdot 2 \cdots (p-1)][(p+1) \cdots (p+p-1)] \cdots \cdots [((m-1)p+1) \cdots ((m-1)p+p-1)].$$

Sugestão: (Para (d)) Por indução sobre s , usando (b) e (c) acima.

2. As Classes Residuais e a sua Aritmética

Seja dado um inteiro $m > 1$. Define-se a *classe residual módulo m* do elemento a de \mathbb{Z} como sendo o conjunto

$$\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

Exemplos

1. Se $m = 2$, então $\bar{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x \text{ é par}\}$ e $\bar{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$. Temos também que $\bar{a} = \bar{0}$, se a é par e $\bar{a} = \bar{1}$, se a é ímpar.

2. Seja $m = 3$. Então

$$\bar{0} = \{3\lambda \mid \lambda \in \mathbb{Z}\}$$

$$\bar{1} = \{3\lambda + 1 \mid \lambda \in \mathbb{Z}\}$$

$$\bar{2} = \{3\lambda + 2 \mid \lambda \in \mathbb{Z}\}$$

e

$$\bar{a} = \begin{cases} \bar{0} & , \text{ se } a \text{ é múltiplo de 3} \\ \bar{1} & , \text{ se } a \text{ tem resto 1 quando dividido por 3} \\ \bar{2} & , \text{ se } a \text{ tem resto 2 quando dividido por 3} \end{cases}$$

Vejamos algumas propriedades das classes residuais.

Proposição 4. *Seja m um inteiro maior do que 1. Temos que*

- (i) $\bar{a} = \bar{b}$ se e somente se $a \equiv b \pmod{m}$;
- (ii) Se $\bar{a} \cap \bar{b} \neq \emptyset$, então $\bar{a} = \bar{b}$;
- (iii) $\bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$.

Demonstração: i. Suponha que $\bar{a} = \bar{b}$, como $a \in \bar{a}$, segue que $a \in \bar{b}$, logo $a \equiv b \pmod{m}$.

Reciprocamente, suponha $a \equiv b \pmod{m}$, logo $x \equiv a \pmod{m}$ se

e somente se $x \equiv b \pmod{m}$ e portanto $x \in \bar{a}$ se e somente se $x \in \bar{b}$, donde $\bar{a} = \bar{b}$.

ii. Suponha que $\bar{a} \cap \bar{b} \neq \emptyset$ e seja $c \in \bar{a} \cap \bar{b}$. Segue que $c \equiv a \pmod{m}$ e $c \equiv b \pmod{m}$, logo $a \equiv b \pmod{m}$ e pelo item (i) segue que $\bar{a} = \bar{b}$.

iii. É claro que $\bigcup_{a \in \mathbb{Z}} \bar{a} \subset \mathbb{Z}$. Por outro lado, seja $x \in \mathbb{Z}$, como $x \in \bar{x}$,

segue que $x \in \bigcup_{a \in \mathbb{Z}} \bar{a}$ e portanto $\mathbb{Z} \subset \bigcup_{a \in \mathbb{Z}} \bar{a}$. \square

Um inteiro qualquer b tal que $\bar{b} = \bar{a}$ é dito *representante* da classe residual \bar{a} .

Exemplos

1. Se $m = 2$, então qualquer inteiro par é representante da classe residual $\bar{0}$ e qualquer inteiro ímpar é representante da classe residual $\bar{1}$;

2. Se $m = 3$, então qualquer múltiplo de 3 é representante da classe residual $\bar{0}$. Temos que $1, 4, 7, 10, -2, -5, -8, -11$, etc, são representantes da classe residual $\bar{1}$ enquanto que $2, 5, -1, -4$, etc, são representantes da classe residual $\bar{2}$.

Proposição 5. *Para cada $a \in \mathbb{Z}$ existe um, e somente um $r \in \mathbb{Z}$ com $0 \leq r < m$ tal que $\bar{a} = \bar{r}$.*

Demonstração: Seja $a \in \mathbb{Z}$. Pela divisão euclidiana existe um único inteiro r com $0 \leq r < m$ tal que $a = m \cdot q + r$ para algum $q \in \mathbb{Z}$. Portanto é único o inteiro r tal que $0 \leq r < m$ e $a \equiv r \pmod{m}$, consequentemente, é único o inteiro r tal que $0 \leq r < m$ e $\bar{a} = \bar{r}$. \square

Corolário. *Existem exatamente m classes residuais módulo m distintas, a saber $\bar{0}, \bar{1}, \dots, \bar{(m-1)}$.*

Um conjunto $\{a_1, \dots, a_m\}$ é chamado de *sistema completo de resíduos módulo m* se para todo $a \in \mathbb{Z}$ existir um i , com $i = 0, \dots, m$, tal que $a \equiv a_i \pmod{m}$.

Em outras palavras, $\{a_1, \dots, a_m\}$ é um sistema completo de resíduos módulo m se e somente se $\bar{a}_1, \dots, \bar{a}_m$ são as m classes residuais módulo m . Os conjuntos $\{0, 1, \dots, m-1\}$ e $\{1, 2, \dots, m\}$ são sistemas

completos de resíduos módulo m . É fácil verificar que m inteiros formam um sistema completo de resíduos módulo m , se e somente se eles são dois a dois incongruentes módulo m .

O conjunto de todas as classes residuais módulo m é representado por \mathbb{Z}_m . Ele possui m elementos que podem ser representados por $\overline{0}, \overline{1}, \dots, \overline{(m-1)}$. A primeira vantagem das classes residuais é que transformam a congruência $a \equiv b \pmod{m}$ na igualdade $\overline{a} = \overline{b}$.

Em \mathbb{Z}_m definimos as seguintes operações:

Adição: $\overline{a} + \overline{b} = \overline{a+b}$

Multiplicação: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Note que sendo definidas estas operações usando os representantes a e b para as classes residuais \overline{a} e \overline{b} respectivamente, temos que verificar que ao mudarmos os representantes das classes \overline{a} e \overline{b} , não mudam os valores de $\overline{a+b}$ e de $\overline{a \cdot b}$. Para verificar que isto acontece, basta notar que se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, então $\overline{a+b} = \overline{a'+b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$, o que segue diretamente dos ítems (iv) e (v) da Proposição 2.

Estas operações que acabamos de definir gozam das seguintes propriedades:

Propriedades da Adição

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos

A₁ (**Associatividade**) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

A₂ (**Comutatividade**) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

A₃ (**Existência de zero**) $\overline{a} + \overline{0} = \overline{a}$ para todo $a \in \mathbb{Z}_m$;

A₄ (**Existência de simétrico**) $\overline{a} + \overline{(-a)} = \overline{0}$.

Propriedades da Multiplicação

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos

M₁ (**Associatividade**) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;

M₂ (**Comutatividade**) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;

M₃ (**Existência de unidade**) $\overline{a} \cdot \overline{1} = \overline{a}$.

Propriedade de Ligação da Multiplicação com a Adição

Para todos $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$, temos

$$\text{AM (Distributividade)} \quad \bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

Todas estas propriedades são fáceis de verificar. Por exemplo, (AM) se prova como segue:

$$\begin{aligned} \bar{a} \cdot (\bar{b} + \bar{c}) &= \overline{\bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}} = \overline{\bar{a} \cdot (b + c)} \\ &= \overline{\bar{a} \cdot b + \bar{a} \cdot c} = \overline{\bar{a} \cdot b} + \overline{\bar{a} \cdot c} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \end{aligned}$$

Temos portanto que \mathbb{Z}_m com as operações acima definidas é um anel. Como a aplicação

$$\begin{array}{rcl} \psi: \mathbb{Z} & \longrightarrow & \mathbb{Z}_m \\ a & \longmapsto & \bar{a} \end{array}$$

é claramente um homomorfismo de anéis, ela é o homomorfismo característico ρ que definimos no Capítulo 3.

Exemplos

1. As tabelas da adição e da multiplicação em $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ são

$+$	$\bar{0}$	$\bar{1}$	
$\bar{0}$	$\bar{0}$	$\bar{1}$	
$\bar{1}$	$\bar{1}$	$\bar{0}$	

\cdot	$\bar{0}$	$\bar{1}$	
$\bar{0}$	$\bar{0}$	$\bar{0}$	
$\bar{1}$	$\bar{0}$	$\bar{1}$	

2. As tabelas da adição e da multiplicação em $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ são

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	

3. Em $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ temos

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

É interessante notar que \mathbb{Z}_4 não é um domínio de integridade pois $\bar{2} \neq \bar{0}$ e no entanto $\bar{2} \cdot \bar{2} = \bar{0}$.

4. Em $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ temos

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Note que $\mathbb{Z}_2, \mathbb{Z}_3$ e \mathbb{Z}_5 com as operações acima definidas são corpos. A seguir damos uma caracterização dos elementos invertíveis de \mathbb{Z}_m .

Proposição 6. Um elemento $\bar{a} \in \mathbb{Z}_m$ é invertível se e somente se $(a, m) = 1$.

Demonstração: Se \bar{a} é invertível, então existe $\bar{b} \in \mathbb{Z}$ tal que $\bar{1} = \bar{a} \cdot \bar{b} = \bar{a} \cdot b$, logo $a \cdot b \equiv 1 \pmod{m}$, isto é, existe um inteiro t tal que $a \cdot b + t \cdot m = 1$, logo $(a, m) = 1$.

Reciprocamente, se $(a, m) = 1$, existem inteiros b e t tais que $a \cdot b + m \cdot t = 1$ e consequentemente, $\bar{1} = a \cdot b + m \cdot t = \bar{a} \cdot \bar{b} + \bar{m} \cdot \bar{t} = \bar{a} \cdot \bar{b} + \bar{0} = \bar{a} \cdot \bar{b}$, portanto \bar{a} é invertível. \square

Corolário. \mathbb{Z}_m é um corpo se e somente se m é primo.

Demonstração: Se \mathbb{Z}_m é um corpo e m não é primo, então $m = m_1 \cdot m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$, logo $\bar{0} = \bar{m} = \bar{m}_1 \cdot \bar{m}_2$ com $\bar{m}_1 \neq 0$ e $\bar{m}_2 \neq 0$, contradição.

Reciprocamente, suponha m primo. Como $(i, m) = 1$ para $i = 1, \dots, m - 1$, segue pela Proposição que $\bar{1}, \bar{2}, \dots, \bar{(m-1)}$ são invertíveis. \square

A seguinte função aritmética desempenha um papel importante na teoria dos números

$$\begin{aligned}\Phi: \mathbb{Z} \setminus \{0, \pm 1\} &\longrightarrow \mathbb{N} \\ n &\longmapsto \text{número de inteiros positivos} \\ &\quad \text{menores do que } |n| \text{ e primos com } n\end{aligned}$$

Esta é chamada de *função Φ de Euler*. Pela Proposição 6, temos que $\Phi(n) =$ número de elementos invertíveis de $\mathbb{Z}_{|n|}$. Estudaremos esta função com mais detalhes na Seção 4.

Um conjunto $\{a_1, \dots, a_{\Phi(m)}\} \subset \mathbb{Z}$ é chamado de *sistema reduzido de resíduos módulo m* se $\bar{a}_1, \dots, \bar{a}_{\Phi(m)}$ são os elementos invertíveis de \mathbb{Z}_m .

Sendo \mathbb{Z}_m^* o conjunto dos elementos invertíveis de \mathbb{Z}_m , temos então que $\mathbb{Z}_m^* = \{\bar{a}_1, \dots, \bar{a}_{\Phi(m)}\}$, onde $\{a_1, \dots, a_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulos m .

Recorde que \mathbb{Z}_m^* é multiplicativamente fechado e que o inverso de todo elemento de \mathbb{Z}_m^* é um elemento de \mathbb{Z}_m^* .

No caso em que p é primo, temos pelo Corolário da Proposição 6, que $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$. Sejam $\bar{1}, \dots, \bar{p-1}$ os elementos de \mathbb{Z}_p^* . Os elementos $\bar{1}$ e $\bar{-1} = \bar{p-1}$ são os únicos elementos de \mathbb{Z}_p^* que são auto-inversos, isto é, são as únicas soluções da equação $x^2 = \bar{1}$. De fato, de $0 = x^2 - \bar{1} = (x - \bar{1})(x + \bar{1})$, e do fato de \mathbb{Z}_p ser um corpo, portanto um domínio de integridade, segue que $x - \bar{1} = 0$ ou $x + \bar{1} = 0$

e consequentemente $x = \bar{1}$ ou $x = \overline{-1}$.

Teorema 1 (Teorema de Wilson). Se p é um número primo positivo, então $(p - 1)! \equiv -1 \pmod p$.

Demonstração: No produto $\bar{1} \cdot \bar{2} \cdots \overline{p-2} \cdot \overline{p-1}$, para cada fator distinto de $\bar{1}$ e de $\overline{-1} = \overline{p-1}$ existe um fator que é o seu inverso, logo $\bar{1} \cdot \bar{2} \cdots \overline{p-2} \cdot \overline{p-1} = \bar{1} \cdot \overline{p-1} = \overline{-1}$. Daí segue que $(p - 1)! = \overline{-1}$, donde $(p - 1)! \equiv -1 \pmod p$.

Problemas

2.1 Seja $\{a_1, \dots, a_m\}$ um sistema completo de resíduos módulo m .

- (a) Mostre que se a é um inteiro, então $\{a_1 + a, \dots, a_m + a\}$ é um sistema completo de resíduos módulo m ;
- (b) Se $(a, m) = 1$, então $\{a \cdot a_1, \dots, a \cdot a_m\}$ é um sistema completo de resíduos módulo m . Mostre que vale a recíproca;
- (c) Se p é primo e a um inteiro que não é múltiplo de p , mostre que $a^{p-1} \equiv 1 \pmod p$ (Pequeno Teorema de Fermat);
- (d) Mostre que se $(r, m) = 1$, então $\{a, a + r, \dots, a + (m - 1)r\}$ é um sistema completo de resíduos módulo m .

Sugestão: (Para (c)) Considere os dois sistemas completos de resíduos $\{0, 1, \dots, p - 1\}$ e $\{0, a \cdot 1, \dots, a(p - 1)\}$ e note que $1 \dots (p - 1) \equiv a^{p-1} \cdot 1 \dots (p - 1) \pmod p$.

2.2 Faça as tabelas da adição e da multiplicação para \mathbb{Z}_6 e \mathbb{Z}_7 .

2.3 Ache os elementos invertíveis de $\mathbb{Z}_6, \mathbb{Z}_7, \mathbb{Z}_8$ e \mathbb{Z}_9 .

2.4 Ache os inversos de

- | | |
|--|--|
| (a) $\bar{5}$ em \mathbb{Z}_6 | (b) $\bar{3}, \bar{4}$ e $\bar{5}$ em \mathbb{Z}_7 |
| (c) $\bar{3}, \bar{5}$, e $\bar{7}$ em \mathbb{Z}_8 | (d) $\bar{5}, \bar{4}$ e $\bar{8}$ em \mathbb{Z}_9 |
| (e) $\overline{1951}$ em \mathbb{Z}_{2431} | (f) $\bar{3}, \bar{5}$ e $\bar{7}$ em \mathbb{Z}_8 |

2.5 (a) Seja $\{a_1, \dots, a_{\Phi(m)}\}$ um sistema reduzido de resíduos módulo m . Mostre que se $(a, m) = 1$, então $\{a \cdot a_1, \dots, a \cdot a_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulo m ;

(b) Mostre a seguinte generalização do Pequeno Teorema de Fermat, devida a Euler. Se $(a, m) = 1$, então $a^{\Phi(m)} \equiv 1 \pmod{m}$.

2.6 (a) Mostre que se n não é primo e $n > 4$, então $(n-1)! \equiv 0 \pmod{n}$;

(b) E se $n = 4$, o que acontece?

(c) Mostre a recíproca do Teorema de Wilson. Se $(n-1)! \equiv -1 \pmod{n}$, então n é primo.

2.7 Seja p um número primo positivo, calcule

$$(a) (p!, (p-1)! - 1) \quad (b) (p!, (p-1)! + 1)$$

Sugestão: Use o Teorema de Wilson.

3. Congruências Lineares

Seja $m > 1$ um inteiro e sejam $\bar{a}, \bar{b} \in \mathbb{Z}_m$, queremos resolver em \mathbb{Z}_m equações do tipo

$$\bar{a} \cdot \bar{x} = \bar{b}, \tag{1}$$

ou seja, resolver em $x \in \mathbb{Z}$ a congruência

$$ax \equiv b \pmod{m} \tag{2}$$

Se x_0 é uma solução de (2) e se $x_1 \equiv x_0 \pmod{m}$, então x_1 é também uma solução de (2), portanto as soluções da congruência (2) se repartem em classes residuais módulo m . Cada classe residual de soluções da congruência (2) é chamada de *solução módulo m* e corresponde a uma solução da equação (1).

Se $(a, m) = 1$, pela Proposição 6 segue que \bar{a} é invertível em \mathbb{Z}_m . Portanto a equação (1) tem neste caso uma única solução dada por

$$\bar{x} = (\bar{a})^{-1} \cdot \bar{b}.$$

Em outras palavras, se $(a, m) = 1$, então a congruência (2) tem uma única solução módulo m .

Teorema 2. *Sejam a, b e m inteiros com m > 1. Seja d = (a, m). Temos*

(i) *A congruência (2) tem solução se e somente se d | b;*

(ii) Se $d \mid b$, existem exatamente d soluções distintas módulo m , cujos representantes são

$$x_0, x_0 + \frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d},$$

onde x_0 é uma solução particular qualquer de (2).

Demonstração: i. A congruência $ax \equiv b \pmod{m}$ admite solução em x se e somente se a equação diofantina $ax + my = b$ admite solução em x e y e isto é, equivalente pelo Teorema 3, Capítulo 5, à condição $d \mid b$.

ii. Seja x_0 uma solução qualquer da congruência $ax \equiv b \pmod{m}$, logo existe y_0 tal que x_0, y_0 é uma solução particular da equação diofantina $ax + my = b$. Pelo Teorema 4, Capítulo 5, temos que toda solução da equação diofantina $ax + my = b$ é, para algum $t \in \mathbb{Z}$, da forma

$$x = x_0 + t\frac{m}{d}, \quad y = y_0 - t\frac{a}{d},$$

portanto toda solução da congruência $ax \equiv b \pmod{m}$ é da forma

$$x = x_0 + t\frac{m}{d}, \quad t \in \mathbb{Z}.$$

Considere agora as seguintes soluções de (2)

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}. \quad (3)$$

Estas são claramente duas a duas incongruentes módulos m , além disso, se $x = x_0 + t\frac{m}{d}$ é uma solução qualquer de (2), pondo $t = dq + r$ com $0 \leq r < d$, temos que

$$x \equiv x_0 + t\frac{m}{d} \equiv x_0 + r\frac{m}{d} \pmod{m},$$

logo x é congruente módulo m a uma das soluções em (3). □

Exemplos

1. Considere a congruência $12x \equiv 28 \pmod{8}$.

Como $d = (12, 8) = 4$ e $4 \mid 28$, temos pelo Teorema 2, (i) que a congruência admite quatro soluções distintas módulo 8. Por inspeção é fácil ver que $x_0 = 3$ é uma solução. Pelo Teorema 2, (ii) temos que

as soluções módulo 8 tem como representantes 3, 5, 7 e 9. Qualquer outra solução da congruência é congruente módulo 8 a uma destas.

2. Considere a congruência $245x \equiv 95 \pmod{180}$.

Como $d = (245, 180) = 5$ e $5 \mid 95$, segue que a congruência admite cinco soluções distintas módulo 180. A nossa congruência, tendo em vista a Proposição 3, (iv), é equivalente a $49x \equiv 19 \pmod{36}$ (as congruências são equivalentes porém as soluções da congruência original são consideradas módulo 180, enquanto que as da outra são módulo 36), da qual devemos achar uma solução particular que pode ser obtida resolvendo a equação diofantina

$$49x - 36y = 19.$$

Pelo método desenvolvido no Capítulo 5, temos

	1	2	1	3	3
49	36	13	10	3	1
13	10	3	1	0	

$$1 = 10 - 3 \cdot 3$$

$$3 = 13 - 1 \cdot 10$$

$$10 = 36 - 2 \cdot 13$$

$$13 = 49 - 1 \cdot 36$$

logo,

$$\begin{aligned} 1 &= 10 - 3 \cdot (13 - 1 \cdot 10) = -3 \cdot 13 + 4 \cdot 10 \\ &= -3 \cdot 13 + 4 \cdot (36 - 2 \cdot 13) = 4 \cdot 36 - 11 \cdot 13 \\ &= 4 \cdot 36 - 11 \cdot (49 - 1 \cdot 36) = -11 \cdot 49 + 15 \cdot 36. \end{aligned}$$

Segue então que

$$19 = -209 \cdot 49 + 285 \cdot 36.$$

Portanto, uma solução particular da equação diofantina é $x_0 = -209$ e $y_0 = -285$. Temos então que $x_0 = -209$ é uma solução particular da congruência $245x \equiv 95 \pmod{180}$. Consequentemente as soluções da congruência módulo 180 tem como representantes

$$-209 + r \cdot 36 , \quad r = 0, 1, 2, 3, 4,$$

ou seja

$$-209, -173, -137, -101, -65,$$

ou ainda

$$151, 7, 53, 79, 115.$$

Problemas

3.1 Resolva as congruências:

- | | |
|----------------------------------|----------------------------------|
| (a) $3x \equiv 5 \pmod{7}$ | (b) $4x \equiv 2 \pmod{3}$ |
| (c) $7x \equiv 21 \pmod{49}$ | (d) $3x \equiv 1 \pmod{6}$ |
| (e) $18x \equiv 12 \pmod{42}$ | (f) $12x \equiv 9 \pmod{15}$ |
| (g) $240x \equiv 148 \pmod{242}$ | (h) $6125x \equiv 77 \pmod{189}$ |

4.2 Resolva os seguintes sistemas de congruências:

$$(a) \begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 3 \pmod{7} \end{cases} \quad (b) \begin{cases} x \equiv 4 \pmod{8} \\ x \equiv 1 \pmod{4} \end{cases}$$

4.3 Em quais condições o sistema de congruências abaixo admite solução

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

4.4 Sob quais condições as seguintes progressões aritméticas com $a, b, r, s \in \mathbb{Z}$, $a_n = a + n \cdot r$ e $b_n = b + n \cdot s$, têm interseção não vazia.

Sugestão: Use o Problema 4.3

4.5 Resolva o sistema de congruências

$$\begin{cases} 2x + 7y \equiv 2 \pmod{5} \\ 3x - y \equiv 1 \pmod{5} \end{cases}$$

4.6 Ache o menor inteiro positivo que deixa restos 2,3 e 2 quando dividido respectivamente por 3,5 e 7.

4. A Função Φ de Euler

Note que a definição da função Φ de Euler dada no parágrafo 2 nos fornece que $\Phi(n) = \Phi(-n)$ para todo $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. É fácil deduzir da definição que $\Phi(p) = p - 1$ se e somente se p é um primo positivo.

Proposição 7. *Se p é um número primo positivo e $n \in \mathbb{N}$, então $\Phi(p^n) = p^{n-1}(p - 1)$.*

Demonstração: O ponto crucial da demonstração é que p sendo primo temos que $(m, p^n) \neq 1$ se e somente se m é um múltiplo de p .

Considere a seqüência

$$1, 2, \dots, p, p + 1, \dots, 2p, \dots, 3p, \dots, p^{n-1} \cdot p.$$

Os inteiros não primos com p^n nesta seqüência, devido à observação acima, são $p, 2p, 3p, \dots, p^{n-1} \cdot p$ que são p^{n-1} em número, donde os inteiros menores do que p^n e primos com p^n são em número $p^n - p^{n-1} = p^{n-1}(p - 1)$.

Proposição 8. *Se m e n são inteiros em $\mathbb{Z} \setminus \{0, \pm 1\}$ tais que $(n, m) = 1$, então $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$.*

Demonstração: Basta claramente demonstrar o resultado para n e m maiores do que 1. Considere a seguinte tabela formada com os inteiros de 1 a $n \cdot m$

1	2	...	k	...	m
$m + 1$	$m + 2$...	$m + k$...	$2m$
\vdots	\vdots		\vdots		\vdots
$(n - 1)m + 1$	$(n - 1)m + 2$...	$(n - 1)m + k$...	$n \cdot m$

Como $(t, n \cdot m) = 1$ se e somente se $(t, m) = 1$ e $(t, n) = 1$ (verifique), devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e com n , para determinar os que são primos com $n \cdot m$.

Se o primeiro elemento de uma coluna não for primo com m , então todos os elementos da coluna não são primos com m . Portanto, os elementos primos com m estão necessariamente nas colunas restantes

que são $\Phi(m)$ em número e é fácil ver que são primos com m todos os elementos destas colunas. Vejamos agora quais são os elementos primos com n em cada uma destas $\Phi(m)$ colunas.

Como $(n, m) = 1$, a seqüência $k, m+k, \dots, (n-1)m+k$ forma um sistema completo de resíduos módulo n (veja Problema 2.1 (d)) e portanto $\Phi(n)$ destes elementos são primos com n . Logo o número de elementos simultaneamente primos com m e n é $\Phi(n) \cdot \Phi(m)$. \square

Corolário. *Se $m = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ com p_1, \dots, p_r primos distintos e $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, então*

$$\begin{aligned}\Phi(m) &= p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1} (p_1 - 1) \cdots (p_r - 1) \\ &= m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

Exemplos

1. $\Phi(100) = \Phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$
2. $\Phi(725) = \Phi(5^2 \cdot 29) = 725 \left(1 - \frac{1}{29}\right) \left(1 - \frac{1}{5}\right) = 560$
3. $\Phi(7^3) = 7^2(7 - 1) = 49 \cdot 6 = 294.$

Do corolário acima é fácil verificar que se $m \neq 0, \pm 1, \pm 2$, então $\Phi(m)$ é par. Os números m para os quais $\Phi(m) = 2^r$, para algum $r \in \mathbb{N}$, são muito importantes e se relacionam, via resultados de Gauss, com a construção com régua e compasso dos polígonos regulares. A proposição seguinte nos permitirá caracterizar tais números.

Proposição 9. *Se $\Phi(m) = 2^r$ para algum $r \in \mathbb{N}$, então a decomposição de m em fatores primos é dada por*

$$m = \pm 2^s \cdot (2^{2^{n_1}} + 1) \cdots (2^{2^{n_k}} + 1),$$

com $s \in \mathbb{Z}^+$ e $n_1, \dots, n_k \in \mathbb{N}$ tais que os $(2^{2^{n_i}} + 1)$ com $i = 1, \dots, k$, são primos distintos.

Demonstração: Seja $m = \pm p_0^{\alpha_0} \cdots p_k^{\alpha_k}$ com p_0, \dots, p_k primos positivos distintos, $\alpha_0 \in \mathbb{Z}^+$ e $\alpha_1, \dots, \alpha_k \in \mathbb{N}$. Vamos supor

$$2 = p_0 < p_1 < \cdots < p_k.$$

Temos então que

$$\Phi(m) = p_0^{\alpha_0-1} p_1^{\alpha_1-1} \cdots p_k^{\alpha_k-1} (p_0 - 1) \cdots (p_k - 1) = 2^r.$$

Como p_1, \dots, p_k são diferentes de 2, devemos ter $\alpha_1 = 1, \dots, \alpha_k = 1$. Além disso, $p_i - 1 = 2^{\beta_i}$ para $i = 1, \dots, k$, logo $p_i = 2^{\beta_i} + 1$ e como p_i é primo segue, da Proposição 2, Capítulo 5, que $\beta_i = 2^{n_i}$ com $n_i \in \mathbb{Z}^+$. Logo, pondo $s = \alpha_0$, temos que

$$m = \pm 2^s(2^{2^{n_1}} + 1) \cdots (2^{2^{n_k}} + 1).$$

Problemas

4.1 Calcule

- (a) $\Phi(125)$ (b) $\Phi(16200)$ (c) $\Phi(2097)$

4.2 Ache os valores de m sabendo que

- (a) $\Phi(m) = 2^2$ (b) $\Phi(m) = 2^3$ (c) $\Phi(m) = 2^4$
 (d) $\Phi(m) = 2^5$ (e) $\Phi(m) = 3^2 \cdot 2$ (f) $\Phi(m) = 10$

5. O Legado de um Gigante

Carl Friedrich Gauss (1777-1855) foi um dos maiores matemáticos de todos os tempos, legando-nos uma imponente obra matemática.

Ainda adolescente Gauss ficou intrigado com o paradoxo do binômio de Newton. A fórmula do binômio

$$(1+x)^\alpha = 1 + \frac{\alpha}{1}x + \frac{\alpha(\alpha-1)}{2!}x^2 + \dots,$$

estendida pelo próprio Newton para valores de α não necessariamente inteiros positivos tem no seu segundo membro uma soma infinita. Estas somas eram tratadas pelos predecessores de Gauss, entre eles o próprio Newton, Leibniz e Euler como se fossem finitas, gerando paradoxos. Por exemplo, pondo $x = -2$ e $\alpha = -1$ na expressão acima obtém-se a igualdade

$$-1 = 1 + 2 + 2^2 + \dots$$

o que é absurdo. Gauss então introduziu o conceito de convergência para as somas infinitas, chamadas séries, provando por exemplo que

se α e x são reais com $|x| < 1$, então a série do binômio de Newton é convergente. O trabalho de Gauss nesta direção teve grande influência sobre seus contemporâneos Abel e Cauchy e sobre os seus sucessores Weierstrass e Dedekind, responsáveis pelo desenvolvimento da Análise Matemática. Este trabalho sobre séries inclui a série hipergeométrica que contém como casos particulares muitas séries importantes, e pode ser considerado como divisor de águas entre o Cálculo Diferencial intuitivo de Newton e Leibniz e o rigor da Análise Matemática.

Aos dezessete anos Gauss se estabeleceu a meta de corrigir e completar o que os seus predecessores haviam feito em Aritmética. Aos 21 anos como fruto deste projeto ele produziu a sua obra prima, o livro “*Disquisitiones Arithmeticae*” que contém grandes contribuições à Aritmética e à Álgebra e que foi publicado em 1801, três anos após a sua conclusão.

No livro, Gauss introduz e estuda as congruências e as equações do tipo

$$x^n \equiv a \pmod{p},$$

isto é, as equações $x^n = \bar{a}$ em \mathbb{Z}_p . Um problema natural neste contexto é saber para quais valores de $a \in \mathbb{Z}$, a equação acima possui solução. Este é um problema difícil e até hoje sem solução. Em busca da solução, Gauss se restringiu ao caso $n = 2$ e elaborou tabelas para compreender o problema. Gauss não conseguiu resolver o problema mas descobriu e demonstrou uma propriedade maravilhosa, detectada anteriormente por Euler, o *Teorema da Reciprocidade Quadrática*, cujo enunciado segue.

Se p e q são números primos positivos distintos, então as congruências

$$x^2 \equiv q \pmod{p} \quad \text{e} \quad x^2 \equiv p \pmod{q},$$

são ambas resolúveis ou ambas não resolúveis exceto quando $p \equiv 3 \pmod{4}$, e neste caso uma e somente uma das congruências admite solução.

Gauss obteve este resultado aos 19 anos e ficou tão intrigado com ele que posteriormente produziu 5 outras demonstrações e estudou os casos $n = 3$ e $n = 4$.

No final do *Disquisitiones*, Gauss aplica a teoria que desenvolveu para atacar a *ciclotomia*, isto é, o estudo das raízes n -ésimas da unidade, e apresenta o seu belo resultado sobre a construtibilidade com régua e compasso de polígonos regulares.

Outra famosa contribuição do Gauss é o chamado Teorema Fundamental da Álgebra, que estabelece que toda equação algébrica com coeficientes reais (ou complexos) admite pelo menos uma raiz complexa. Este é outro teorema que fascinou Gauss dando-lhe ao longo da vida quatro provas distintas.

Outras áreas onde Gauss deixou contribuições relevantes foram, Estatística (distribuição normal de Gauss), Geometria (geometria das superfícies e geometrias não euclidianas) e Física (magnetismo). Mas de todo este universo Gauss nunca escondeu a sua preferência sintetizada na seguinte frase,

“A matemática é a rainha das ciências e a aritmética é a rainha da matemática”

Anéis

A teoria dos Anéis é um dos principais assuntos do vasto campo da Álgebra abstrata. A origem da Álgebra remonta aos babilônios e o seu desenvolvimento percorreu um longo caminho que não pretendemos retratar aqui mas que teve um momento importante no século 16 com os matemáticos da chamada Escola de Bolonha que se ocuparam da resolução das equações algébricas do terceiro e do quarto grau. Em seguida Bombelli deu um passo decisivo introduzindo o simbolismo apropriado para as operações permitindo a manipulação de expressões e fórmulas. Um outro momento importante para a Álgebra ocorreu na primeira metade do século 19 com os trabalhos do irlandês Hamilton e de seus contemporâneos ingleses. Hamilton introduziu o formalismo dos números complexos que é até hoje usado e posteriormente definiu formalmente os quaternios dando mais um passo decisivo para o desenvolvimento da Álgebra abstrata. Importante para o desenvolvimento da teoria foi o estudo dos anéis de inteiros algébricos iniciado por Gauss e desenvolvido por Kummer, Dedekind, Kronecker Dirichlet e Hilbert no final do século 19, início do século 20. Finalmente, a noção abstrata de anel foi introduzida na segunda década do século 20.

1. Anéis

Retomamos aqui os conceitos de anel, subanel e homomorfismo introduzidos no Capítulo 2. O próximo resultado nos fornece um modo ligeiramente mais econômico do que usar a definição para verificar que um dado subconjunto A' de A é um subanel de A .

Proposição 1. Sejam A um anel e A' um subconjunto de A . Temos que A' é um subanel de A se e somente se as seguintes condições são satisfeitas

$$(i) \quad 1 \in A';$$

$$(ii) \quad \text{Quaisquer que sejam } a, b \in A', \text{ temos que } a - b \in A' \text{ e } a \cdot b \in A'.$$

Demonstração: É claro que se A' é um subanel de A , então as condições (i) e (ii) são satisfeitas. Suponha agora que tais condições sejam verificadas. Como $1 \in A'$, segue que $0 = 1 - 1 \in A'$. Se $a \in A'$, então $-a = 0 - a \in A'$.

Sejam agora a e b elementos de A' , logo $-b \in A'$ e consequentemente

$$a + b = a - (-b) \in A'.$$

Como $a \cdot b \in A'$ e as demais propriedades que definem um anel são verificadas em A' pois o são em A , temos que A' é um subanel de A . \square

Proposição 2. Seja A um anel. Se $\{A_i\}_{i \in I}$ é uma família de subanéis de A , então $\bigcap_{i \in I} A_i$ é um subanel de A .

Demonstração: Como $1 \in A_i$ para todo $i \in I$, segue que $1 \in \bigcap_{i \in I} A_i$.

Sejam agora $a, b \in \bigcap_{i \in I} A_i$, logo $a, b \in A_i$ para todo $i \in I$ e portanto para todo $i \in I$, temos que $a - b \in A_i$ e $a \cdot b \in A_i$. Consequentemente,

$$a - b \in \bigcap_{i \in I} A_i \quad \text{e} \quad a \cdot b \in \bigcap_{i \in I} A_i$$

e o resultado segue da Proposição 1. \square

Proposição 3. Seja B um anel e sejam A um subanel de B e $b_1, \dots, b_n \in B \setminus \{0\}$. O conjunto $A[b_1, \dots, b_n]$ de todos os elementos de B que são somas de elemento da forma $a \cdot b^{r_1} \cdots b_n^{r_n}$ com $a \in A$ e $r_1, \dots, r_n \in \mathbb{Z}^+$, é um subanel de B que contém A e b_1, \dots, b_n .

Demonstração: É claro que $1 \in A[b_1, \dots, b_n]$ pois $1 = 1 \cdot b_1^0 \cdots b_n^0$. Por outro lado, é claro que se $x, y \in A[b_1, \dots, b_n]$, então $x - y$ e $x \cdot y$

estão em $A[b_1, \dots, b_n]$. Consequentemente pela Proposição 1, temos que $A[b_1, \dots, b_n]$ é um subanel de B . Como para todo $a \in A$, temos que $a = a \cdot b_1^0 \cdots b_n^0$ e que $b_i = 1 \cdot b_1^0 \cdots b_i^1 \cdots b_n^0$ para todo i , então $A[b_1, \dots, b_n]$ contém A e b_1, \dots, b_n . \square

O anel $A[b_1, \dots, b_n]$ é chamado de *subanel de B gerado por A e por b_1, \dots, b_n* . É fácil verificar que $A[b_1, \dots, b_n]$ é o menor subanel de B que contém A e b_1, \dots, b_n , no sentido que todo subanel de B que contém A e b_1, \dots, b_n também contém $A[b_1, \dots, b_n]$. É também fácil verificar que $A[b_1, \dots, b_n]$ é a interseção de todos os subanéis de B que contém A e b_1, \dots, b_n .

Um subconjunto K' de um corpo K será chamado de *subcorpo* de K , se K' é um subanel de K e é um corpo. Portanto K' é um subanel de K tal que o inverso de todo elemento de $K' \setminus \{0\}$ pertence a K' . Quando K' é um subcorpo de K dizemos que K é uma extensão de K' .

Seja K' um subcorpo de um corpo K . Se $b_1, \dots, b_n \in K \setminus \{0\}$ então $K'[b_1, \dots, b_n]$ é um subanel de K e portanto também domínio de integridade, logo possuindo um corpo de frações que se identifica naturalmente com o conjunto $K'(b_1, \dots, b_n)$ de todos os elementos de K que são frações com numerador em $K'[b_1, \dots, b_n]$ e denominador em $K'[b_1, \dots, b_n] \setminus \{0\}$. Temos claramente que $K'(b_1, \dots, b_n)$ é o menor subcorpo de K que contém K' e b_1, \dots, b_n .

Dados dois anéis A e B é possível dotar o produto cartesiano $A \times B$ de uma estrutura natural de anel onde as operações de adição e de multiplicação são dadas por

$$\begin{aligned}(a, b) + (a', b') &= (a + a', b + b') \\ (a, b) \cdot (a', b') &= (a \cdot a', b \cdot b')\end{aligned}$$

Proposição 4. *Se A e B são anéis, então o conjunto $A \times B$ com as operações acima definidas é um anel.*

Demonstração: A comutatividade e a associatividade da adição e da multiplicação são de verificação fácil a partir das definições, o mesmo ocorrendo com a distributividade da multiplicação com relação à adição. O elemento zero da adição é $(0,0)$, o simétrico de (a, b) é $(-a, -b)$ e $(1,1)$ é o elemento identidade da multiplicação. \square

Proposição 5. Um elemento $(a, b) \in A \times B$ é invertível se e somente se a é invertível em A e b é invertível em B . Neste caso, temos que $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Demonstração: Suponha (a, b) invertível com inverso (c, d) , logo

$$(1, 1) = (a, b) \cdot (c, d) = (a \cdot c, b \cdot d),$$

portanto $a \cdot c = 1$ e $b \cdot d = 1$. Consequentemente a e b são invertíveis com $c = a^{-1}$ e $d = b^{-1}$.

Reciprocamente, se a e b são invertíveis, então

$$(a, b) \cdot (a^{-1}, b^{-1}) = (a \cdot a^{-1}, b \cdot b^{-1}) = (1, 1),$$

consequentemente (a, b) é invertível e $(a, b)^{-1} = (a^{-1}, b^{-1})$. \square

Usando a notação A^* para representar o conjunto dos elementos invertíveis do anel A , a Proposição 5 nos afirma que

$$(A \times B)^* = A^* \times B^*$$

Sejam A um anel e S um conjunto não vazio. Definimos A^S como sendo o conjunto de todas as funções de S em A e nele consideramos as seguintes operações de adição e de multiplicação

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x)\end{aligned}$$

Proposição 6. Sejam A um anel e S um conjunto não vazio qualquer. O conjunto A^S com as operações acima definidas é um anel.

Demonstração: A associatividade e comutatividade da adição e da multiplicação bem como a distributividade da multiplicação com relação à adição são fáceis de verificar. O elemento zero da adição é a função constante $0: S \rightarrow A$ que associa a cada $x \in S$ o elemento $0 \in A$, enquanto que o elemento identidade da multiplicação é a função constante $1: S \rightarrow A$ que associa a cada $x \in S$ o elemento $1 \in A$. O simétrico de $f: S \rightarrow A$ é a função $-f: S \rightarrow A$ tal que $(-f)(x) = -f(x)$. \square

Exemplo: Seja A um anel, o conjunto $A^{\mathbb{N}}$ de todas as seqüências de A é um anel com as operações acima definidas. Este anel será denotado também por $S(A)$.

Problemas

1.1 Mostre que o subanel $\mathbb{Z}[1/2]$ de \mathbb{Q} é igual a $\left\{ \frac{a}{2^n} \mid a \in \mathbb{Z} \text{ e } n \in \mathbb{Z}^+ \right\}$ juntamente com a adição e multiplicação de números racionais.

1.2 Se A é um subanel de B e $b_1, \dots, b_n \in B \setminus \{0\}$. Mostre que $A[b_1, \dots, b_n]$ é o menor subanel de B que contém A e b_1, \dots, b_n . Mostre também que $A[b_1, \dots, b_n]$ é a interseção de todos os subanéis de B que contém A e b_1, \dots, b_n .

1.3 Demonstre com detalhes as Proposições 4 e 6.

1.4 Mostre que o único subanel de \mathbb{Z} é ele próprio.

1.5 Seja S um conjunto com um único elemento. Mostre que se A é um anel, então A^S é isomorfo a A .

1.6 Seja S um conjunto com dois elementos. Mostre que se A é um anel, então A^S é isomorfo a $A \times A$.

1.7 Seja p um número primo. Mostre que

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, p \nmid n \right\}$$

é um subanel de \mathbb{Q} . Quais são os elementos invertíveis de $\mathbb{Z}_{(p)}$? Determine o corpo quociente de $\mathbb{Z}_{(p)}$.

1.8 Sejam A um anel e S um conjunto não vazio. Determine os divisores de zero de A^S (isto é, os elementos $f \in A^S$ para os quais existem $g \in A^S \setminus \{0\}$ tais que $f \cdot g = 0$).

2. Homomorfismos e Ideais

As próximas proposições nos relacionarão os subanéis e ideais de dois anéis A e B em presença de um homomorfismo $f: A \rightarrow B$.

Proposição 7. Seja $f: A \rightarrow B$ um homomorfismo de anéis. Temos que

- (i) Se A' é um subanel de A , então $f(A')$ é um subanel de $f(A)$;
- (ii) Se B' é um subanel de B , então $f^{-1}(B')$ é um subanel de A .

Demonstração: i. Isto segue da Proposição 8, Capítulo 2, tomando no lugar de f a restrição de f a A' .

ii. Seja B' um subanel de B . Como $f(1) = 1 \in B'$, segue que $1 \in f^{-1}(B')$. Além disso, se $a, b \in f^{-1}(B')$, segue que $f(a), f(b) \in B'$. Portanto

$$f(a - b) = f(a) - f(b) \in B'$$

e

$$f(a \cdot b) = f(a) \cdot f(b) \in B'$$

logo $a - b \in f^{-1}(B')$ e $a \cdot b \in f^{-1}(B')$. Portanto pela Proposição 1 temos que $f^{-1}(B')$ é um subanel de A . \square

Proposição 8. Seja $f: A \rightarrow B$ um homomorfismo de anéis. Temos que

- (i) Se I é um ideal de A , então $f(I)$ é um ideal de $f(A)$;
- (ii) Se J é um ideal de B , então $f^{-1}(J)$ é um ideal de A .

Demonstração: i. Se I é um ideal de A , então $I \neq \emptyset$, logo $f(I) \neq \emptyset$. Suponha agora que $a', b' \in f(I)$, logo $a' = f(a)$ e $b' = f(b)$ com $a, b \in I$.

Consequentemente,

$$a' + b' = f(a) + f(b) = f(a + b) \in f(I).$$

Agora, se $a' \in f(I)$ e $b' \in f(I)$, temos que $a' = f(a)$ e $b' = f(b)$ com $a \in I$ e $b \in I$, logo $a \cdot b \in I$ e consequentemente,

$$a' \cdot b' = f(a) \cdot f(b) = f(a \cdot b) \in f(I).$$

Temos portanto que $f(I)$ é um ideal de $f(A)$.

ii. Como $0 \in J$ e $f(0) = 0$, segue que $0 \in f^{-1}(J)$ e portanto $f^{-1}(J) \neq \emptyset$. Suponha agora que $a, b \in f^{-1}(J)$, logo $f(a), f(b) \in J$, portanto

$$f(a + b) = f(a) + f(b) \in J,$$

e consequentemente $a + b \in f^{-1}(J)$. Por outro lado, se $a \in A$ e $b \in f^{-1}(J)$, então

$$f(a \cdot b) = f(a) \cdot f(b) \in J,$$

e portanto $a \cdot b \in f^{-1}(J)$. Temos então que $f^{-1}(J)$ é um ideal de A .

□

No caso em que $J = (0)$, o ideal $f^{-1}(J)$ é chamado de *núcleo* de f e é denotado por $N(f)$. Em outras palavras,

$$N(f) = \{a \in A \mid f(a) = 0\}.$$

Se A é um subanel de B e J é um ideal de B então a proposição aplicada ao homomorfismo inclusão $i: A \rightarrow B$, $i(x) = x$, nos diz que $J \cap A$ é um ideal de A .

Proposição 9. *Seja $f: A \rightarrow B$ um homomorfismo de anéis. Temos que*

- (i) $f(a') = f(a)$ se e somente se $a' - a \in N(f)$;
- (ii) f é injetora se e somente se $N(f) = (0)$.

Demonstração: i. $f(a') = f(a)$ se e somente se $f(a' - a) = f(a') - f(a) = 0$ se e somente se $a' - a \in N(f)$.

ii. Segue imediatamente de (i). □

Corolário. *Seja $f: K \rightarrow B$ um homomorfismo de anéis, onde K é um corpo. Então f é injetora.*

Demonstração: Como $N(f)$ é um ideal de K e os únicos ideais de K são (0) e o próprio K (veja Problema 2.1, Capítulo 4) e como $N(f) \neq K$ pois $f(1) = 1 \neq 0$, segue que $N(f) = (0)$. Logo o resultado segue da proposição. □

Um ideal I de um anel A com $I \neq A$ é chamado de *ideal primo* se toda vez que $a \cdot b \in I$ com $a, b \in A$, segue que $a \in I$ ou $b \in I$.

Um ideal M de A com $M \neq A$ é chamado de *ideal maximal* se para todo ideal I tal que $M \subsetneq I \subset A$, temos que $I = A$.

Proposição 10. *Todo ideal maximal é primo.*

Demonstração: Seja M um ideal maximal de um anel A e sejam a e b elementos de A tais que $a \cdot b \in M$. Se $a \notin M$, então temos que

o ideal $M + I(a)$ é tal que $M \subsetneq M + I(a) \subset A$, logo $M + I(a) = A$. Portanto existem $m \in M$ e $\lambda \in A$ tais que

$$1 = m + \lambda \cdot a$$

Multiplicando ambos os membros da igualdade acima por b , temos que

$$b = m \cdot b + \lambda \cdot a \cdot b \in M,$$

pois $m, a \cdot b \in M$. Isto prova que M é primo. \square

Proposição 11. *Num domínio principal A , são equivalentes para um ideal I com $I \neq (0)$ e $I \neq A$ as seguintes afirmações*

- (i) I é maximal;
- (ii) I é primo;
- (iii) $I = I(p)$, onde p é um elemento primo de A .

Demonstração: A implicação (i) \Rightarrow (ii) segue da Proposição 10.

Vamos provar (ii) \Rightarrow (iii). Suponha que $I \neq (0)$ é um ideal primo de A . Como A é principal, então existe $p \in A$ tal que $I = I(p)$. É claro que $p \neq 0$ e p é não invertível. Suponha que $p \mid a \cdot b$, logo $a \cdot b \in I(p)$ e como $I(p)$ é primo temos que $a \in I(p)$ ou $b \in I(p)$ e portanto $p \mid a$ ou $p \mid b$. Portanto p é primo.

Para provar que (iii) \Rightarrow (i), seja $I = I(p)$ o ideal gerado por um elemento primo p de A . Suponha que $J = I(a)$ seja um ideal de A tal que $I(p) \subsetneq J \subset A$. Temos que $a \mid p$ e a não é associado de p ; como p é primo, segue que a é invertível e portanto $J = I(a) = A$. \square

Problemas

2.1 Seja $h: A \rightarrow B$ uma função não nula de anéis tal que $h(a \cdot b) = h(a) \cdot h(b)$ quaisquer que sejam $a, b \in A$. Mostre que se B é um domínio então $h(1) = 1$.

2.2 Mostre que a função

$$\begin{aligned} f: \mathbb{Z} &\longrightarrow \mathbb{Z}_{12} \\ x &\longmapsto \overline{9x} \end{aligned}$$

é tal que, para todo $a, b \in \mathbb{Z}$, $f(a+b) = f(a)+f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$ e $f(1) \neq 1$.

2.3 Sejam A um anel e $a \in A$.

- a) Mostre que o ideal (0) é primo se e somente se A é um domínio;
- b) Mostre que a é primo em A se e somente se $I(a)$ é um ideal primo de A .

2.4 Seja $f: A \rightarrow B$ um homomorfismo. Mostre que

- a) Se J é um ideal primo de B , então $f^{-1}(J)$ é um ideal primo de A ;
- b) Se I é um ideal primo de A contendo $N(f)$, então $f(I)$ é um ideal primo de $f(A)$.

2.5 Seja $f: A \rightarrow B$ um homomorfismo de anéis e sejam I e J respectivamente ideais de A e B .

- a) Mostre que $f(f^{-1}(J)) = J \cap f(A)$;
- b) Mostre que $f^{-1}(f(I)) = I + N(f)$.

2.6 Dado um homomorfismo de anéis $f: A \rightarrow B$, mostre que é uma bijeção a aplicação,

$$\begin{array}{ccc} \psi: \{\text{ideais de } A \text{ que contém } N(f)\} & \longrightarrow & \{\text{ideais de } f(A)\}, \\ I & \longmapsto & f(I) \end{array}$$

e que esta bijeção faz corresponder os ideais primos de cada conjunto.

Sugestão: Use os Problemas 2.4 e 2.5.

2.7 Seja m um inteiro maior do que 1 e seja $\rho: \mathbb{Z} \rightarrow \mathbb{Z}_m$ o homomorfismo característico.

- a) Mostre que \mathbb{Z}_m é o único subanel dele próprio;
- b) Seja $J \subset \mathbb{Z}_m$ um ideal e considere a aplicação inversa de ψ relativa a ρ do Problema 2.6. Mostre que $J = I(\bar{\lambda})$ onde λ é um divisor de m . Isto prova que \mathbb{Z}_m é um anel principal e que os seus ideais estão em correspondência bijetora com os divisores positivos de m .

2.8 Sejam S um conjunto não vazio e A um anel. Se $T \subset S$, mostre que $\{f \in A^S \mid f(T) \subset \{0\}\}$ é um ideal de A^S . Mostre que este ideal é primo se e somente se A é um domínio e T possui um só elemento.

2.9 Sejam S um subconjunto de um anel A e $a \in A$. Define-se

$$aS = \{a \cdot x \mid x \in S\}.$$

Mostre que $\{a \in A \mid aS = \{0\}\}$ é um ideal de A .

2.10 a) Sejam A um anel e I um ideal de A . Mostre que se todo elemento de $A \setminus I$ for invertível, então I é o único ideal maximal de A . Um anel que possui um único ideal maximal é chamado de *anel local*;

b) Mostre que o anel $\mathbb{Z}_{(p)}$ do Problema 1.7 é local com ideal maximal

$$M_p \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, p \mid m \text{ e } p \nmid n \right\}$$

3. Anéis Quocientes

A relação de congruência em \mathbb{Z} estudada no Capítulo 6 pode ser reinterpretada em termos de ideais como segue,

$$a \equiv b \pmod{n} \iff b - a \in I(n).$$

Portanto, generalizando o que fizemos para as congruências, suponha que A é um anel e I um ideal de A , define-se a seguinte relação binária em A ,

$$a \equiv b \pmod{I} \iff b - a \in I.$$

Prova-se facilmente (faça-o) que esta relação é uma relação de equivalência em A satisfazendo à seguinte propriedade.

Proposição 12. Se $a \equiv b \pmod{I}$ e $c \equiv d \pmod{I}$, então $a + c \equiv b + d \pmod{I}$ e $a \cdot c \equiv b \cdot d \pmod{I}$.

Demonstração: Semelhante à demonstração da Proposição 2 do Capítulo 6 e a deixamos como exercício. \square

Sejam A um anel, I um ideal de A e $a \in A$. Define-se a classe residual de a módulo I como sendo o conjunto

$$\bar{a} = a + I = \{a + x \mid x \in I\}.$$

O elemento a é chamado de *representante* da classe residual \bar{a} , e tal como para as congruências (e mais geralmente para qualquer relação de equivalência), estas classes satisfazem às seguintes condições (compare com a Proposição 4 do Capítulo 6)

$$(1) \quad \bar{a} = \bar{b} \iff a \equiv b \pmod{I};$$

$$(2) \quad \bar{a} \cap \bar{b} \neq \emptyset \implies \bar{a} = \bar{b};$$

$$(3) \quad \bigcup_{a \in A} \bar{a} = A.$$

Denotaremos por A/I o conjunto das classes residuais módulo I de todos os elementos de A . Por exemplo, se $A = \mathbb{Z}$ e $I = I(m)$ para algum inteiro m maior do que 1, então $A/I = \mathbb{Z}_m$.

Define-se em A/I as seguintes operações,

Adição: $\bar{a} + \bar{b} = \overline{a + b}$

Multiplicação: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Novamente, tal como no caso das congruências mostra-se facilmente (faça-o) que as leis acima definem efetivamente operações em A/I e que quando $I \neq A$ tem-se que A/I com estas operações é um anel, chamado *anel quociente* de A por I .

Neste anel, o elemento zero é $\bar{0} = I$, o simétrico de $\bar{a} = a + I$ é $\overline{(-a)} = -a + I$, o elemento unidade é $\bar{1} = 1 + I$. A aplicação

$$\begin{aligned} \varphi: A &\longrightarrow A/I \\ a &\longmapsto \bar{a} \end{aligned}$$

define um homomorfismo sobrejetor cujo núcleo é I .

Proposição 13 (Teorema do Isomorfismo). *Seja dado um homomorfismo sobrejetor $h: A \rightarrow B$. Existe um isomorfismo $\tilde{h}: A/N(h) \rightarrow B$ tal que $h = \tilde{h} \circ \varphi$.*

Demonstração: Para $a \in A$, definimos $\tilde{h}(\bar{a}) = h(a)$. Temos que mostrar que o valor de $\tilde{h}(\bar{a})$ depende apenas da classe \bar{a} e não do representante a da classe. Suponha que $\bar{a} = \bar{b}$, logo $a - b \in N(h)$ e portanto pela Proposição 9 temos que $h(a) = h(b)$, mostrando que

$\tilde{h}(\bar{a}) = \tilde{h}(\bar{b})$. A função \tilde{h} é um homomorfismo pois

$$\begin{aligned}\tilde{h}(\bar{a} + \bar{b}) &= \tilde{h}(\overline{a+b}) = h(a+b) = h(a) + h(b) = \tilde{h}(\bar{a}) + \tilde{h}(\bar{b}), \\ \tilde{h}(\bar{a} \cdot \bar{b}) &= \tilde{h}(\overline{a \cdot b}) = h(a \cdot b) = h(a) \cdot h(b) = \tilde{h}(\bar{a}) \cdot \tilde{h}(\bar{b}),\end{aligned}$$

e $\tilde{h}(\bar{1}) = h(1) = 1$. A função \tilde{h} é sobrejetora pois se $y \in B$, existe $x \in A$ tal que $h(x) = y$ (pois h é sobrejetora), logo $\tilde{h}(\bar{x}) = h(x) = y$. É claro que

$$\tilde{h}(\bar{a}) = 0 \iff h(a) = 0 \iff a \in N(h) \iff \bar{a} = \bar{0}$$

logo $N(\tilde{h}) = \{\bar{0}\}$ e portanto pela Proposição 9, \tilde{h} é injetora. Temos então que \tilde{h} é bijetora e verifica trivialmente a igualdade $h = \tilde{h} \circ \varphi$.

□

Corolário. Seja $h: A \rightarrow B$ um homomorfismo, então $A/N(h)$ e $h(A)$ são anéis isomorfos.

Demonstração: Substitua B por $h(A)$ e use a proposição. □

Usando o homomorfismo identidade $Id: A \rightarrow A$, vê-se que $A/(0)$ é isomorfo a A .

Proposição 14. Sejam A um anel e I um ideal de A com $I \neq A$. Temos que

- (i) A/I é um domínio se e somente se I é ideal primo;
- (ii) A/I é um corpo se e somente se I é ideal maximal.

Demonstração: (i) Suponha que A/I é um domínio. Suponha que $a \cdot b \in I$, logo $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{0}$, consequentemente, temos que $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$ e portanto $a \in I$ ou $b \in I$ ou seja, I é primo.

Reciprocamente, suponha que I é um ideal primo. Sejam $\bar{a}, \bar{b} \in A/I$ tais que $\bar{a} \cdot \bar{b} = \bar{0}$, logo $a \cdot b \in I$ e portanto $a \in I$ ou $b \in I$, ou seja $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

(ii) Suponha que A/I seja um corpo e suponha que J seja um ideal tal que $I \subsetneq J \subset A$. Seja $a \in J \setminus I$, logo $\bar{a} \neq \bar{0}$ e portanto existe $\bar{b} \in A/I$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$, isto é, $a \cdot b - 1 \in I$. Como $I \subset J$ e $a \cdot b \in J$ (pois $a \in J$), segue que $1 \in J$ e consequentemente, $J = A$.

Reciprocamente, suponha que I seja um ideal maximal. Seja $\bar{a} \neq \bar{0}$, isto é, $a \notin I$, temos que $I \subsetneq I + I(a)$, logo $I + I(a) = A$ e portanto $1 = b + \lambda \cdot a$ com $b \in I$, $\lambda \in A$ e consequentemente $I = \bar{0} + \bar{\lambda} \cdot \bar{a} = \bar{\lambda} \cdot \bar{a}$. Isto prova que \bar{a} é invertível e portanto A/I é um corpo. \square

Note que a proposição acima nos fornece outra prova de que todo ideal maximal é primo já que todo corpo é domínio.

Sejam A um anel e $\rho: \mathbb{Z} \rightarrow A$ o homomorfismo característico. Sendo \mathbb{Z} principal temos que $N(\rho) = I(n)$ para algum $n \in \mathbb{Z}^+$, $n \neq 1$. O inteiro n assim definido é chamado de *característica* de A e denotado por $\text{car}(A)$. Pelo corolário do Teorema do Isomorfismo (Proposição 13), temos que $\rho(\mathbb{Z})$ é isomorfo a $\mathbb{Z}_n = \mathbb{Z}/I(n)$ (note que $\mathbb{Z}_0 = \mathbb{Z}/(0) = \mathbb{Z}$), logo \mathbb{Z}_n pode ser visto como subanel de A e é o menor subanel de A . Se A é um domínio, então $\rho(\mathbb{Z})$ é um domínio e portanto $\mathbb{Z}/I(n)$ é um domínio. Isto só é verificado quando $n = 0$ ou n é um número primo (veja Proposição 14 e Problema 2.3). Portanto a característica de um domínio ou é zero ou é um número primo.

Sejam $\rho: \mathbb{Z} \rightarrow A$ o homomorfismo característico e A' um subanel de A . Como $1 \in A'$, temos que $\rho(\mathbb{Z}) \subset A'$. Portanto $\rho(\mathbb{Z})$ é o menor subanel de A . Daí segue em particular que a característica de qualquer subanel de A é igual à característica de A .

Seja K um corpo de característica > 0 . Como K é um domínio de integridade, a sua característica é um número primo p , então K contém o corpo $\rho(\mathbb{Z}) \simeq \mathbb{Z}_p$. Além disso, $\rho(\mathbb{Z})$ é o menor subcorpo de K , chamado de *corpo primo* de K e denotado por K_0 .

Se K é um corpo de característica zero, então o homomorfismo característico ρ é injetor, logo pela Proposição 10, Capítulo 2, existe um homomorfismo de anéis

$$\tilde{\rho}: \mathbb{Q} \rightarrow K.$$

Como \mathbb{Q} é um corpo, temos que $\tilde{\rho}$ é um homomorfismo injetor (veja o Corolário da Proposição 9). Se K' é um subcorpo de K , então $\mathbb{Q} \simeq \tilde{\rho}(\mathbb{Q}) \subset K'$ e portanto $\tilde{\rho}(\mathbb{Q})$ é o menor subcorpo de K , chamado de *corpo primo* de K e denotado por K_0 .

Exemplos

1. Como $\rho: \mathbb{Z} \rightarrow \mathbb{Z}$ e $\rho: \mathbb{Z} \rightarrow \mathbb{Q}$ são injetoras, temos que $\text{car}(\mathbb{Z}) = \text{car}(\mathbb{Q}) = 0$. Mais geralmente, se A é um anel ordenado, pela Proposição 5 do Capítulo 3, temos que $\text{car}(A) = 0$.
2. Seja $n \in \mathbb{N}$ com $n > 1$. Como $N(\rho) = I(n)$, onde ρ é o homomorfismo característico de \mathbb{Z} em \mathbb{Z}_n , temos que $\text{car}(\mathbb{Z}_n) = n$.
3. Seja $\rho: \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}$. É claro que ρ é injetora, logo $\text{car}(\mathbb{Z}_2 \times \mathbb{Z}) = 0$.
4. Seja $\rho: \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$. Temos que $\rho(1), \rho(2), \rho(3), \rho(4), \rho(5) \neq 0$ e $\rho(6) = 0$, logo $N(\rho) = I(6)$ (justifique). Portanto $\text{car}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$.

O próximo resultado possui várias aplicações.

Teorema 1. *Sejam A um domínio principal e $a_1, \dots, a_n \in A \setminus A^*$. Considere o homomorfismo*

$$\begin{aligned} h: A &\longrightarrow A/I(a_1) \times \cdots \times A/I(a_n) \\ a &\longmapsto (\bar{a}_1, \dots, \bar{a}_n) \end{aligned}$$

Temos que

- (i) $N(h) = I(m)$, onde m é um mínimo múltiplo comum de a_1, \dots, a_n ;
- (ii) Se para todo i, j com $i \neq j$, tem-se que a_i e a_j são primos entre si, então h é sobrejetora.

Demonstração: i. Como $h(a) = 0 \iff a \in I(a_1) \cap \cdots \cap I(a_n)$, segue que $N(h) = I(a_1) \cap \cdots \cap I(a_n)$, e portanto $N(h) = I(m)$ com m um mmc de a_1, \dots, a_n (veja Problema 2.7, Capítulo 4).

ii. Ponha $b = a_1 \dots a_n$. É claro que sendo a_i e a_j primos entre si para $i \neq j$, tem-se que b_i e a_i são primos entre si, onde $b_i = \frac{b}{a_i}$. Logo existem $r_i, s_i \in A$ tais que

$$r_i a_i + s_i b_i = 1 \quad (1)$$

Dado $(\bar{c}_1, \dots, \bar{c}_n) \in A/I(a_1) \times \cdots \times A/I(a_n)$, como $a_i | b_j$ se $i \neq j$, temos que

$$a = c_1 s_1 b_1 + \cdots + c_n s_n b_n,$$

é tal que

$$a \equiv c_i s_i b_i \pmod{a_i} \quad (2)$$

De (1) temos que

$$s_i b_i \equiv 1 \pmod{a_i},$$

logo de (2) segue que

$$a \equiv c_i \pmod{a_i}.$$

Consequentemente,

$$h(a) = (\bar{c}_1, \dots, \bar{c}_n),$$

provando assim que h é sobrejetora. \square

Corolário 1. Se $a_1, \dots, a_n \in \mathbb{Z}^+ \setminus \{1\}$, então

$$\text{car } (\mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}) = \text{mmc}(a_1, \dots, a_n).$$

Corolário 2. Se A é um domínio principal e $a_1, \dots, a_n \in A \setminus A^*$ são dois a dois primos entre si, então

$$A/I(a_1 \cdots a_n) \simeq A/I(a_1) \times \dots \times A/I(a_n).$$

Demonstração: Note que a hipótese implica que $a_1 \dots a_n$ é um mmc de a_1, \dots, a_n e o resultado segue do Teorema e da Proposição 13. \square

Seja Φ a função Φ de Euler. Temos o seguinte

Corolário 3. Se $m, n \in \mathbb{Z} \setminus \{0, \pm 1\}$ com $(m, n) = 1$, então $\Phi(m \cdot n) = \Phi(m)\Phi(n)$.

Demonstração: Pelo Corolário 2, temos um isomorfismo $\mathbb{Z}_{n \cdot m} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$. Como isomorfismos estabelecem uma bijeção entre os elementos invertíveis de cada anel e como os elementos invertíveis de $\mathbb{Z}_m \times \mathbb{Z}_n$ são os pares ordenados cujas primeiras componentes são elementos invertíveis de \mathbb{Z}_m e as segundas componentes elementos invertíveis de \mathbb{Z}_n (veja Proposição 5), segue que $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$. \square

O Corolário 3 acima nos dá uma outra demonstração da Proposição 8 do Capítulo 6.

Problemas

3.1 Sejam A um domínio, $a \in A$ e $n \in \mathbb{Z}$. Mostre que $na = 0$ se somente se $a = 0$ ou $\text{car}(A) | n$.

3.2 a) Mostre que se A é um domínio de característica $p > 0$ e se $q = p^\alpha$ para algum $\alpha \in \mathbb{N}$, então para todo $x, y \in A$, temos que

$$(x + y)^q = x^q + y^q$$

b) Mostre que

$$\begin{aligned} F_q: A &\longrightarrow A \\ x &\longmapsto x^q \end{aligned}$$

é um homomorfismo injetor. Se A é finito, conclua que F_q é um isomorfismo.

Sugestão: Use o Corolário 3 do Teorema 2, Capítulo 3 para provar a segunda parte de (b).

3.3 Seja A um domínio com corpo de frações K . Mostre que

$$\text{car}(K) = \text{car}(A).$$

3.4 Sejam A e B anéis de características respectivamente n e m . Mostre que

$$\text{car}(A \times B) = \text{mmc}(m, n).$$

3.5 Mostre que todo anel ordenado tem característica zero. Conclua que todo anel ordenado é infinito.

Sugestão: Use a Proposição 5, Capítulo 3.

3.6 Sejam $m_1, m_2 \in \mathbb{Z}^+ \setminus \{1\}$ primos entre si. Sejam $a_1, a_2 \in \mathbb{Z}$. Mostre que o sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

possui soluções inteiras e que estas são todas congruentes entre si módulo $\text{mmc}(m_1, m_2)$.

Os Números Reais

Realizaremos neste capítulo a construção dos números reais dando ênfase aos seus aspectos algébricos. No final do capítulo faremos a conexão com a Análise Matemática através do chamado Princípio do Supremo.

Aproximadamente dois milênios e meio se passaram desde a descoberta pelos pitagóricos da irracionalidade de $\sqrt{2}$ até a construção rigorosa dos números reais realizada pela escola alemã na segunda metade do século dezenove.

Ao descobrir a existência dos números irracionais os pitagóricos viram ruir a sua crença de que os números inteiros eram suficientes para tratar os problemas matemáticos. Cerca de um século depois, Eudoxo (408-355 A.C) criava a sua teoria das proporções para fundamentar o uso das grandezas irracionais em geometria. Os trabalhos de Eudoxo foram expostos por Euclides nos Elementos e é praticamente tudo que existe na direção da conceituação dos números reais até o século dezenove.

A preocupação com os fundamentos dos números reais só voltou na primeira metade do século dezenove motivada pelo desenvolvimento da Análise Matemática realizado principalmente por Gauss, Abel e Cauchy. A teoria foi ultimada na segunda metade daquele século com duas construções diferentes dos números reais realizadas por Cantor e Dedekind. Os dois métodos tem em comum apenas o ponto de partida, o corpo ordenado dos números racionais. O método de Cantor, que aqui adotamos, se baseia no uso de seqüências de números racionais, enquanto que o de Dedekind se baseia na noção

de corte nos racionais. A compreensão dos números reais propiciou o impressionante desenvolvimento da Análise Matemática registrado nestes últimos cem anos.

1. Seqüências Convergentes

Nesta seção introduziremos as definições e resultados básicos sobre as seqüências convergentes num corpo ordenado K , preparando o terreno para a construção dos números reais. Daqui por diante K será um corpo ordenado, portanto de característica zero (Veja Problema 3.5, Capítulo 7).

Um elemento do anel $S(K)$ das seqüências de K será denotado por x ou por (x_n) . Usaremos também a seguinte notação:

$$K_+^* = \{x \in K \mid x > 0\}.$$

Uma seqüência $x = (x_n) \in S(K)$ será dita *convergente em K* quando existir um elemento $a \in K$ tal que, para todo $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ com a propriedade,

$$|x_n - a| < \varepsilon , \quad \forall n > N.$$

Um elemento a como acima, se existir, será chamado de *limite* da seqüência x . Neste caso diremos também que a seqüência x *converge para a* .

Relacionado com esta definição temos o seguinte resultado

Proposição 1. *Uma seqüência convergente possui um único limite.*

Demonstração: Suponha por absurdo que a e b sejam dois limites distintos de x . Portanto, dado $\varepsilon \in K_+^*$ existem N_1 e N_2 em \mathbb{N} tais que

$$|x_n - a| < \varepsilon , \quad \forall n > N_1 \quad \text{e} \quad |x_n - b| < \varepsilon , \quad \forall n > N_2.$$

Tomando $N \geq \max\{N_1, N_2\}$, temos que

$$|x_n - a| < \varepsilon \quad \text{e} \quad |x_n - b| < \varepsilon , \quad \forall n > N,$$

logo pela Proposição 4 do Capítulo 2, temos que se $n > N$, então

$$|b - a| = |x_n - a + b - x_n| \leq |x_n - a| + |x_n - b| < 2\varepsilon.$$

Portanto para todo $\varepsilon \in K_+^*$ temos que $|b - a| < 2\varepsilon$. Como $a \neq b$, temos que $|b - a| > 0$, logo tomando $\varepsilon = \frac{1}{2}|b - a|$, segue que $|b - a| < |b - a|$, absurdo. \square

No caso em que x é uma seqüência cujo limite é a , escrevemos

$$\lim x = a,$$

ou ainda

$$\lim_{n \rightarrow \infty} x_n = a.$$

Denotando por $S_c(K)$ o subconjunto de $S(K)$ das seqüências convergentes, a proposição acima nos garante que é bem definida a aplicação

$$\begin{aligned} \lim: S_c(K) &\longrightarrow K \\ x &\longmapsto \lim x \end{aligned}$$

Uma seqüência que não é convergente será dita *divergente*.

Seja $a \in K$, denotaremos também por a a seqüência constante $x_n = a$ para todo $n \in \mathbb{N}$. Podemos então considerar por meio desta identificação K como subanel de $S(K)$. É claro que $\lim a = a$. Segue imediatamente das definições que a seqüência x converge para a se e somente se a seqüência $x - a$ converge para zero.

Denotaremos por $S_0(K)$ o subconjunto de $S_c(K)$ das *seqüências nulas*, isto é, das seqüências que convergem para zero.

Exemplos

1. A seqüência x em $S(\mathbb{Q})$ definida por $x_n = \frac{1}{n}$ converge para zero. De fato, dado $\varepsilon \in \mathbb{Q}_+^*$, tome N um inteiro maior do que $\frac{1}{\varepsilon}$, o que é possível pela propriedade arquimediana de \mathbb{Q} (veja Problema 2.6, Capítulo 2). Temos para $n > N$ que

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} < \frac{1}{N} < \varepsilon.$$

2. A seqüência definida por $x_n = (-1)^n$ é divergente em qualquer corpo ordenado K (justifique).

Uma seqüência $x = (x_n) \in S(K)$ será dita *limitada superiormente* (respectivamente, *inferiormente*) se existir $L \in K$ tal que para todo $n \in \mathbb{N}$ se tenha $x_n \leq L$ (respectivamente, $L \leq x_n$). Uma seqüência limitada superiormente e inferiormente será dita *limitada*. Segue imediatamente da definição que $x = (x_n)$ é limitada se e somente se existe $B \in K_+^*$ tal que $|x_n| \leq B$ para todo $n \in \mathbb{N}$. O subconjunto de $S(K)$ das seqüências limitadas será denotado por $S_\ell(K)$.

Proposição 2. *Toda seqüência convergente é limitada.*

Demonstração: Suponha que $\lim x = a$, logo dado $\varepsilon = 1$, existe um número natural N tal que se $n > N$, então $|x_n - a| < 1$. Como $|x_n| - |a| < |x_n - a|$, temos que se $n > N$, então $|x_n| - |a| < 1$ e consequentemente, $|x_n| < 1 + |a|$. Pondo

$$B = \max\{|x_1|, \dots, |x_N|, 1 + |a|\},$$

temos para todo $n \in \mathbb{N}$ que $|x_n| \leq B$. Portanto x é limitada. \square

Proposição 3. *Sejam $x, y \in S_c(K)$. Então $x + y$ e $x - y$ pertencem a $S_c(K)$ e*

$$\lim(x \pm y) = (\lim x) \pm (\lim y).$$

Demonstração: Suponha que $\lim x = a$ e $\lim y = b$. Dado $\varepsilon \in K_+^*$, existem N_1 e N_2 em \mathbb{N} tais que

$$|x_n - a| < \frac{\varepsilon}{2}, \quad \forall n > N_1,$$

e

$$|y_n - b| < \frac{\varepsilon}{2}, \quad \forall n > N_2.$$

Seja $N = \max\{N_1, N_2\}$, logo se $n > N$, temos que

$$\begin{aligned} |x_n \pm y_n - (a \pm b)| &= |(x_n - a) \pm (y_n - b)| \\ &\leq |x_n - a| + |y_n - b| < \varepsilon, \end{aligned}$$

provando o resultado. \square

Da Proposição segue imediatamente o seguinte corolário

Corolário. *Se $x, y \in S_c(K)$ são tais que $\lim x = \lim y$, então $x - y$ é uma seqüência nula.*

Proposição 4. Sejam $x, y \in S(K)$. Se x é limitada e y é uma seqüência nula, então $x \cdot y$ é uma seqüência nula.

Demonstração: Como x é limitada, existe $B \in K_+^*$ tal que $|x_n| \leq B$ para todo $n \in \mathbb{N}$. Como $\lim y = 0$, temos que dado $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que

$$|y_n| = |y_n - 0| < \frac{\varepsilon}{B} , \quad \forall n > N.$$

Portanto para $n > N$, temos que

$$|x_n y_n - 0| = |x_n| |y_n| < B \frac{\varepsilon}{B} = \varepsilon,$$

provando assim o resultado. \square

Proposição 5. Sejam $x, y \in S(K)$. Se x e y são convergentes, então $x \cdot y$ é convergente e $\lim(x \cdot y) = (\lim x) \cdot (\lim y)$.

Demonstração: Suponha que $\lim x = a$ e $\lim y = b$. Vamos provar que a seqüência $x \cdot y - a \cdot b$ converge para zero. De fato, como y é convergente, pela Proposição 2 ela é limitada. Por outro lado a seqüência $x - a$ converge para zero. Portanto pela Proposição 4 temos que

$$\lim(x - a) \cdot y = 0$$

De modo análogo conclui-se que

$$\lim a \cdot (y - b) = 0.$$

Usando as duas igualdades acima, a Proposição 3 e a igualdade

$$x \cdot y - a \cdot b = (x - a) \cdot y + a \cdot (y - b),$$

segue que

$$\lim(x \cdot y - a \cdot b) = 0$$

\square

Teorema 1. Seja K um corpo ordenado. Então $S_c(K)$ é um subanel de $S(K)$ e $\lim: S_c(K) \rightarrow K$ é um homomorfismo sobrejetor de anéis cujo núcleo é $S_0(K)$.

Demonstração: Os fatos que $S_c(K)$ é um subanel de $S(K)$ e que \lim é um homomorfismo seguem das Proposições 3 e 5. É claro que \lim é sobrejetor e que seu núcleo é $S_0(K)$. \square

Corolário. $S_c(K)/S_0(K) \cong K$.

Demonstração: Isto é consequência direta do Teorema 1 e do Teorema do Isomorfismo (Proposição 13, Capítulo 7). \square

Uma seqüência $x = (x_n) \in S(K)$ será dita *monótona crescente* (respectivamente, *monótona decrescente*) se para todos n e m em \mathbb{N} tais que $n \geq m$, se tenha $x_n \geq x_m$ (respectivamente, $x_n \leq x_m$).

Uma seqüência $y \in S(K)$ será chamada de *subseqüência* de uma seqüência $x \in S(K)$, se existir uma seqüência injetora e monótona crescente $i: \mathbb{N} \rightarrow \mathbb{N}$ tal que $y = x \circ i$. Temos portanto que $y_n = x_{i_n}$. Uma classe especial de subseqüências de x é dada pela composição com as translações

$$\begin{aligned}\tau_r: \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n + r\end{aligned}$$

para algum $r \in \mathbb{N}$.

Proposição 6. Seja $x \in S_c(K)$. Então para toda seqüência $i: \mathbb{N} \rightarrow \mathbb{N}$ injetora e monótona crescente, tem-se que $x \circ i \in S_c(K)$ e

$$\lim x \circ i = \lim x.$$

Demonstração: Suponha que $\lim x = a$, logo dado $\varepsilon \in K_+^*$ existe N_1 tal que

$$|x_m - a| < \varepsilon, \quad \forall m > N_1.$$

Como i é injetora e monótona crescente, temos que existe $N \in \mathbb{N}$ tal que $i_n > N_1, \quad \forall n > N$. Portanto, temos que

$$|x_{i_n} - a| < \varepsilon, \quad \forall n > N,$$

o que implica que $x \circ i \in S_c(K)$ e que $\lim x \circ i = \lim x$. \square

A proposição acima nos diz que toda subseqüência de uma seqüência convergente é convergente e o seu limite é igual ao limite da seqüência.

Problemas

1.1 Mostre que $S_\ell(K)$ é um subanel de $S(K)$.

1.2 Mostre que $S_0(K)$ é um ideal de $S_\ell(K)$.

1.3 Sejam $i, j: \mathbb{N} \rightarrow \mathbb{N}$ duas seqüências injetoras e monótonas crescentes. Considere

$$\begin{aligned} i^*: S(K) &\longrightarrow S(K) \\ x &\longmapsto x \circ i \end{aligned}$$

- a) Mostre que i^* é um homomorfismo de anéis
- b) Determine o núcleo de i^*
- c) Mostre que $i^*(S_c(K)) = S_c(K)$ e que $i^*(S_\ell(K)) = S_\ell(K)$
- d) Mostre que $(i \circ j)^* = j^* \circ i^*$.

1.4 Seja $a \in K$ e defina

$$S_a(K) = \{x \in S_c(K) \mid \lim x = a\}.$$

Mostre que $S_a(K) = a + S_0(K)$ e que ao variar de $a \in K$, os conjuntos $S_a(K)$ percorrem todas as classes laterais de $S_0(K)$ em $S_c(K)$.

1.5 Seja $x = (x_n) \in S(K)$, defina $|x|$ como sendo a seqüência $(|x_n|)$. Mostre que se $x \in S_c(K)$, então $|x| \in S_c(K)$ e que $\lim |x| = |\lim x|$.

1.6 Sejam $x, y \in S_c(K)$ e suponha que existe $N \in \mathbb{N}$ tal que

$$x_n \geq y_n \quad , \quad \forall n > N.$$

Mostre que $\lim x \geq \lim y$.

2. Corpos Arquimedianos

Seja K um corpo ordenado. A restrição a \mathbb{N} do homomorfismo característico ρ de K é uma seqüência denotada por ρ . Diremos que K é um *corpo arquimédiano* se a seqüência ρ não for limitada.

Lema 1. K é um corpo arquimédiano se e somente se, quaisquer que sejam $a, b \in K$ com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração: Suponha que K seja arquimédiano e sejam $a, b \in K$ com $b \neq 0$. Então existe $m \in \mathbb{N}$ tal que $m > \left| \frac{a}{b} \right|$, logo $m|b| > |a| \geq a$. Portanto $nb > a$, onde $n = \pm m$ segundo se $b > 0$ ou $b < 0$. A recíproca é imediata. \square

Exemplos

1. O corpo ordenado \mathbb{Q} é arquimédiano (Ver Problema 2.6, Capítulo 2).
2. Exemplo de um corpo ordenado não arquimédiano. Vamos admitir que o leitor esteja familiarizado com os polinômios que serão estudados detalhadamente no Volume 2.

Seja $\mathbb{Q}[x]$ o conjunto dos polinômios numa indeterminada x com coeficientes em \mathbb{Q} . Com a adição e multiplicação de polinômios, $\mathbb{Q}[x]$ é um domínio de integridade. Se

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x] \setminus \{0\}$$

com $a_n \neq 0$, chamamos a_n de *coeficiente líder* de $p(x)$ e o denotamos por $CL(p(x))$. Define-se o coeficiente líder do polinômio zero como sendo zero, isto é, $CL(0) = 0$. É fácil verificar que a seguinte relação em $\mathbb{Q}[x]$,

$$p(x) \leq q(x) \iff CL(q(x) - p(x)) \geq 0,$$

é uma relação de ordem, munindo $\mathbb{Q}[x]$ de uma estrutura de anel ordenado.

Seja $\mathbb{Q}(x)$ o corpo de frações do domínio $\mathbb{Q}[x]$. Pelo Teorema 2 do Capítulo 2, $\mathbb{Q}(x)$ é um corpo ordenado. Observe agora que para todo $n \in \mathbb{N}$, temos em $\mathbb{Q}(x)$ que $n! < x$, logo $\mathbb{Q}(x)$ não é arquimédiano.

O seguinte resultado nos fornecerá uma caracterização importante dos corpos arquimedanos.

Proposição 7. *Seja K um corpo ordenado com corpo primo K_0 . As seguintes asserções são equivalentes.*

- (i) K é arquimédiano;
- (ii) Dados $a, b \in K$ quaisquer, com $a < b$, então existe $r \in K_0$ tal que

$$a < r < b$$

- (iii) Todo elemento de K é limite de uma seqüência em K_0 .

Demonstração: (i) \implies (ii): Sendo K arquimédiano e $b - a \neq 0$, pelo Lema 1 existe $n \in \mathbb{Z}$ tal que

$$n(b - a) > 1.$$

Como $b - a > 0$, é claro que $n > 0$ e portanto

$$\frac{1}{n} < b - a \quad (1)$$

Por outro lado, seja

$$S = \{x \in \mathbb{Z} \mid x > na\}.$$

Pelo fato de \mathbb{K} ser arquimediano temos que $S \neq \emptyset$. Temos também que S é limitado inferiormente pois se $\ell \in \mathbb{Z}$ é tal que $\ell > -a$, temos para todo $x \in S$ que

$$x > na > -n\ell,$$

e portanto $x > -n\ell$ (recordar que o homomorfismo característico é ordenado).

Seja $m = \min S$ (que existe pelo PBO). Temos então que $m > na$, isto é

$$\frac{m}{n} > a, \quad (2)$$

e $(m - 1) < na$, isto é

$$\frac{(m - 1)}{n} < a \quad (3)$$

Segue então de (1), (2) e (3) que

$$a < \frac{m}{n} = \frac{(m - 1)}{n} + \frac{1}{n} < a + \frac{1}{n} < a + b - a = b,$$

e o resultado segue tomando $r = \frac{m}{n}$.

(ii) \implies (iii) Seja $a \in \mathbb{K}$. Para cada $n \in \mathbb{N}$, temos por hipótese que existe $r_n \in K_0$ tal que

$$a - \frac{1}{n} < r_n < a + \frac{1}{n},$$

isto é,

$$|a - r_n| < \frac{1}{n}.$$

Seja $\varepsilon \in K_+^*$, logo de (ii) existe $\varepsilon' \in K_0$ tal que $0 < \varepsilon' < \varepsilon$.

Como $\varepsilon' \in K_0$ e K_0 é ordenadamente isomorfo a \mathbb{Q} que é arquimédiano, temos que existe $N \in \mathbb{N}$ tal que

$$\frac{1}{n1} < \varepsilon' , \quad \forall n > N.$$

Temos então que

$$|a - r_n| < \frac{1}{n1} < \varepsilon' < \varepsilon , \quad \forall n > N,$$

e consequentemente $(r_n) \in S(K_0)$ e $\lim_{n \rightarrow \infty} r_n = a$.

(iii) \Rightarrow (i) Dado $a \in K$, devemos mostrar que existe $m \in \mathbb{N}$ tal que

$$a < m1.$$

De fato, seja $(r_n) \in S(K_0)$ tal que

$$\lim_{n \rightarrow \infty} r_n = a + 1.$$

Agora, dado $\varepsilon = \frac{1}{2}$, existe $N \in \mathbb{N}$ tal que

$$|r_n - (a + 1)| < \frac{1}{2} , \quad \forall n > N,$$

portanto,

$$a < (a + 1) - \frac{1}{2} < r_{N+1} \tag{4}$$

Como K_0 é arquimédiano, existe $m \in \mathbb{N}$ tal que $r_{N+1} < m1$, logo de (4) segue que $a < m1$, provando assim o resultado. \square

Problemas

2.1 Seja K um corpo arquimédiano e sejam $a, b \in K_+^*$. Mostre que existe um e somente um inteiro positivo m tal que

$$(m - 1)a \leq b < ma.$$

Sugestão: Considere o conjunto $S = \{n \in \mathbb{N} \mid na > b\}$. Mostre que $S \neq \emptyset$ e tome $m = \min S$.

2.2 Seja $x = (x_n) \in S(K)$ a seqüência definida por

$$x_n = \frac{1}{n1} , \quad \forall n \in \mathbb{N}.$$

- a) Mostre que se K é arquimediano, então x converge para zero.
- b) Mostre que se $K = \mathbb{Q}(x)$, então a seqüência x não converge para zero.

2.3 Seja K um corpo arquimediano e sejam $b, c \in K$ com $b > 1$. Mostre que existe $n \in \mathbb{N}$ tal que $b^n > c$.

Sugestão: Adapte à presente situação a demonstração do Corolário do Teorema 5, Capítulo 3.

2.4 Seja K um corpo arquimediano. Mostre que se $a \in K$ com $|a| < 1$, então $\lim_{n \rightarrow \infty} a^n = 0$.

Sugestão: Analise separadamente os casos $a = 0$ e $a \neq 0$. Se $a \neq 0$, use Problema 2.3 para mostrar que dado $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que $1/|a|^N > 1/\varepsilon$. Aplique a definição de limite observando que a seqüência $(|a|^n)$ é monótona decrescente.

2.5 Uma série num corpo ordenado K é uma soma infinita

$$a_1 + a_2 + \cdots + a_n + \cdots,$$

com os a_i em K . Diremos que a série é convergente, se for convergente a seqüência $s = (s_n)$ definida por

$$s_n = a_1 + a_2 + \cdots + a_n.$$

A soma da série é por definição o limite da seqüência s .

Suponha que K seja arquimediano. Sejam $a, q \in K$ com $|q| < 1$. Mostre que a série geométrica

$$a + aq + aq^2 + \cdots$$

converge para $\frac{a}{1-q}$.

Sugestão: Use o problema 1.7, Capítulo 3 para escrever compactamente s_n e calcule $\lim_{n \rightarrow \infty} s_n$, usando o Problema 2.4.

2.6 Calcule a soma da seguinte série em \mathbb{Q} ,

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$

3. Seqüências Fundamentais

Nesta seção como no resto do capítulo todos os corpos considerados são corpos ordenados.

Um corpo L será dito uma *extensão ordenada* de um corpo K se L é uma extensão de K tal que a restrição da ordenação de L a K coincide com a ordenação de K .

Na primeira seção do presente capítulo estabelecemos um isomorfismo entre um corpo K e o anel quociente $S_c(K)/S_0(K)$ (veja o Corolário do Teorema 1), o que nos permite identificar, a menos de seqüências nulas de racionais, um número racional com uma seqüência convergente de racionais. Mais precisamente, se $x \in \mathbb{Q}$ e x é uma seqüência de \mathbb{Q} tal que $\lim x = x$, então identifica-se x com $\bar{x} = x + S_0(\mathbb{Q})$. Desenvolvendo esta idéia, Cantor idealizou a seguinte estratégia para ampliar o corpo dos números racionais a fim de obter o corpo dos números reais. A idéia consiste em definir um número real como sendo uma classe residual módulo $S_0(\mathbb{Q})$ de uma seqüência de \mathbb{Q} de um tipo especial, mais precisamente, de uma seqüência de \mathbb{Q} que possa convergir em alguma extensão ordenada de \mathbb{Q} .

Seja L um corpo. Uma seqüência $x = (x_n) \in S(L)$ será chamada de *seqüência fundamental* ou *seqüência de Cauchy* em L se o valor absoluto da diferença entre dois termos da seqüência tende a zero à medida que os seus índices aumentam. Formalmente isto se expressa como segue:

$x = (x_n) \in S(L)$ é uma seqüência fundamental em L se para todo $\varepsilon \in L_+^*$, existe $N \in \mathbb{N}$ tal que, para todos $m, n \in \mathbb{N}$ com $m, n > N$, temos

$$|x_m - x_n| < \varepsilon.$$

É claro que se $x \in S(K)$ é fundamental em alguma extensão ordenada L de K , então ela é fundamental em K .

O próximo resultado nos fornecerá a relação entre seqüências convergentes e fundamentais

Proposição 8. *Toda seqüência convergente é fundamental.*

Demonstração: Seja $x = (x_n) \in S_c(K)$ e suponha que $\lim x = x$.

Temos então que para todo $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que se $m, n > N$, então

$$|x_n - x| < \frac{\varepsilon}{2} \quad \text{e} \quad |x_m - x| < \frac{\varepsilon}{2}.$$

Segue então que se $m, n > N$, temos

$$|x_n - x_m| = |x_n - a - (x_m - a)| \leq |x_n - a| + |x_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

logo x é fundamental em K . \square

A proposição acima nos fornece uma condição necessária, em termos de propriedades intrínsecas, para que uma seqüência $x \in S(K)$ seja convergente em alguma extensão ordenada de K . A condição é a seguinte: Se $x \in S(K)$ é tal que para alguma extensão ordenada L de K a seqüência x é convergente em L , então x é fundamental em K .

Exemplo. A seqüência $x = (x_n) \in S(\mathbb{Q})$ definida por $x_n = (-1)^n$, é não fundamental, logo não converge em nenhuma extensão de \mathbb{Q} .

O próximo resultado nos dará um critério útil para que uma seqüência definida num corpo arquimédiano seja fundamental.

Proposição 9. *Seja K um corpo arquimédiano. Toda seqüência monótona crescente e limitada superiormente de K é fundamental em K .*

Demonstração: Seja $x = (x_n) \in S(K)$ uma seqüência monótona crescente e limitada superiormente. Seja $c \in K$ tal que

$$x_n \leq c \quad , \quad \forall n \in \mathbb{N}.$$

Seja $\varepsilon \in K_+^*$ e considere o conjunto

$$S = \left\{ z \in \mathbb{Z}^+ \mid z \leq \frac{c - x_n}{\varepsilon}, \quad \forall n \in \mathbb{N} \right\}.$$

Como K é arquimédiano, S é limitado superiormente pois caso contrário, existiria $z \in S$ tal que $z > \frac{c - x_1}{\varepsilon}$, absurdo. S é não vazio pois $0 \in S$. Segue então, pela formulação equivalente (PBO') do Princípio da Boa Ordenação, que S possui um maior elemento que denotaremos por r . Como $r \in S$ e $r + 1 \notin S$, temos que

$$r\varepsilon \leq c - x_n \quad , \quad \forall n \in \mathbb{N}$$

e existe $N \in \mathbb{N}$ tal que

$$c - x_N < (r + 1)\varepsilon.$$

Portanto, se $m, n > N$, temos pelas desigualdades acima e pelo fato que x é monótona crescente, que

$$c - x_m \leq c - x_N < (r + 1)\varepsilon \leq c - x_n + \varepsilon,$$

logo

$$|x_n - x_m| = x_n - x_m < \varepsilon,$$

e portanto a seqüência x é fundamental em K . \square

A fim de dar um exemplo de uma seqüência fundamental que não é convergente, considere a seqüência $r = (\alpha_n)$ de K definida recorrentemente como segue

$$\alpha_1 = 1 \quad , \quad \alpha_{n+1} = \frac{4\alpha_n}{2 + \alpha_n^2} \quad , \quad \forall n \geq 1.$$

Lema 2. Para todo $n \in \mathbb{N}$, temos que $\alpha_n^2 < 2$ e $\alpha_n \geq 1$.

Demonastração: Por indução sobre n . O resultado vale trivialmente para $n = 1$.

Suponha que $\alpha_n^2 < 2$ e $\alpha_n \geq 1$, logo

$$\alpha_{n+1}^2 = \frac{16\alpha_n^2}{(2 + \alpha_n^2)^2} = \frac{16\alpha_n^2}{(2 - \alpha_n^2)^2 + 8\alpha_n^2} < \frac{16\alpha_n^2}{8\alpha_n^2} = 2,$$

e

$$\alpha_{n+1} = \frac{4\alpha_n}{2 + \alpha_n^2} \geq \frac{4}{2 + 2} = 1. \quad \square$$

Proposição 10. A seqüência r é fundamental.

Demonastração: Pelo Lema 2 segue que r é limitada superiormente. De fato, $\alpha_n^2 < 2 < 4$, logo $\alpha_n < 2$. Além disso, r é monótona crescente pois

$$\alpha_{n+1} - \alpha_n = \frac{\alpha_n(2 - \alpha_n^2)}{2 + \alpha_n^2} > 0.$$

Segue então pela Proposição 9 que r é fundamental. \square

A seqüência r não é convergente em $K = \mathbb{Q}$, pois se fosse convergente com $\lim r = \alpha \in \mathbb{Q}$, teríamos

$$\lim[\alpha_{n+1}(2 + \alpha_n^2)] = \lim 4\alpha_n,$$

logo pelas Proposições 3, 5 e 6 seguiria que

$$\alpha(2 + \alpha^2) = 4\alpha.$$

Observando que $\alpha \neq 0$ (pois $\alpha_n \geq 1$ para todo $n \in \mathbb{N}$), segue que $\alpha^2 = 2$, o que não é possível para $\alpha \in \mathbb{Q}$. O nosso objetivo será o de ampliar o corpo \mathbb{Q} de modo que a seqüência r passe a ter limite, obtendo assim um corpo contendo $\sqrt{2}$.

Proposição 11. *Toda seqüência fundamental é limitada.*

Demonstração: Seja $x = (x_n)$ uma seqüência fundamental. Tomando $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que para todo $n > N$, tem-se que

$$|x_n| - |x_{N+1}| \leq |x_n - x_{N+1}| < 1.$$

Logo

$$|x_n| < 1 + |x_{N+1}| , \quad \forall n > N,$$

pondendo $B = \max\{|x_1|, \dots, |x_N|, 1 + |x_{N+1}|\}$, segue que

$$|x_n| \leq B , \quad \forall n \in \mathbb{N},$$

logo x é limitada. \square

O conjunto das seqüências fundamentais em K será denotado por $S_f(K)$.

Proposição 12. *$S_f(K)$ é um subanel de $S(K)$.*

Demonstração: Note que toda seqüência constante é fundamental.

Em particular, a seqüência $a_n = 1, \forall n \in \mathbb{N}$, pertence a $S_f(K)$.

Sejam $x, y \in S_f(K)$. Pela Proposição 11, as seqüências x e y são limitadas, logo existe $B \in K_+^*$ tal que

$$|x_n| \leq B \quad \text{e} \quad |y_n| \leq B , \quad \forall n \in \mathbb{N}.$$

Dado $\varepsilon \in K_+^*$, existe N tal que se $m, n > N$, então

$$|x_m - x_n| < \frac{\varepsilon}{2B} \quad \text{e} \quad |y_m - y_n| < \frac{\varepsilon}{2B}.$$

Segue então que

$$\begin{aligned} |x_m y_m - x_n y_n| &= |x_m(y_m - y_n) + y_n(x_m - x_n)| \\ &\leq |x_m| |y_m - y_n| + |y_n| |x_m - x_n| \\ &\leq B \frac{\varepsilon}{2B} + B \frac{\varepsilon}{2B} = \varepsilon. \end{aligned}$$

Temos então que $x \cdot y = (x_n \cdot y_n)$ é fundamental em K .

Por outro lado, dado $\varepsilon \in K_+^*$, existe N tal que se $m, n > N$, então

$$|x_m - x_n| \leq \frac{\varepsilon}{2} \quad \text{e} \quad |y_m - y_n| \leq \frac{\varepsilon}{2},$$

logo se $m, n > N$, temos que

$$|x_m - y_m - (x_n - y_n)| \leq |x_m - x_n| + |y_n - y_m| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

Temos então que $x - y = (x_n - y_n)$ é fundamental em K .

Pela Proposição 1 do Capítulo 7, $S_f(K)$ é um subanel de $S(K)$. □

Proposição 13. *O conjunto $S_0(K)$ das seqüências nulas de K forma um ideal de $S_f(K)$.*

Demonstração: Isto segue do fato que a soma de duas seqüências nulas é claramente uma seqüência nula e que o produto de uma seqüência nula por uma seqüência limitada é uma seqüência nula (Proposição 4) e que toda seqüência fundamental é limitada (Proposição 11). □

A próxima proposição nos será de grande utilidade

Proposição 14. *Seja $x = (x_n) \in S_f(K) \setminus S_0(K)$. Então existem $c \in K_+^*$ e $N \in \mathbb{N}$ tais que $|x_n| > c$, $\forall n > N$.*

Demonstração: A afirmação $x \notin S_0(K)$ significa que existe $a \in K_+^*$ tal que para todo $N \in \mathbb{N}$, existe $\ell > N$ para o qual $|x_\ell| \geq a$.

Como $x \in S_f(K)$, dado $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que se $m, n > N$, então

$$\|x_n - x_m\| \leq |x_n - x_m| < \varepsilon.$$

Logo para $m, n > N$, temos que

$$|x_m| - \varepsilon < |x_n|. \quad (1)$$

Escolha um $\varepsilon \in K_+^*$ tal que $\varepsilon < a$, de modo que pondo $c = a - \varepsilon$, temos que $c \in K_+^*$. Seja N o inteiro para o qual (1) vale para $m, n > N$. Seja ℓ o inteiro maior do que N tal que $|x_\ell| \geq a$, logo de (1), para todo $n > N$, temos que

$$|x_n| > |x_\ell| - \varepsilon \geq a - \varepsilon = c. \quad \square$$

Teorema 2. *O anel quociente $S_f(K)/S_0(K)$ é um corpo.*

Demonstração: Para provar o resultado temos que mostrar que todo elemento \bar{x} não nulo do anel quociente $S_f(K)/S_0(K)$ é invertível. Devemos então provar que dado $x \in S_f(K) \setminus S_0(K)$, existe $y \in S_f(K)$ tal que $x \cdot y - 1 \in S_0(K)$.

De fato, sendo $x \in S_f(K) \setminus S_0(K)$, temos pela Proposição 14 que existem $c \in K_+^*$ e $N' \in \mathbb{N}$ tais que

$$|x_n| > c, \quad \forall n > N'.$$

Tem-se em particular que $x_n \neq 0, \forall n > N'$. Defina $y \in S(K)$ tal que

$$y_n = \begin{cases} 1 & , \text{ se } x_n = 0 \\ x_n^{-1} & , \text{ se } x_n \neq 0 \end{cases}$$

É claro que o produto $x_n \cdot y_n$ vale 1, exceto para apenas um número finito de índices n , quando vale zero. Logo é claro que

$$x \cdot y - 1 \in S_0(K).$$

Só falta agora provar que $y \in S_f(K)$. De fato, dado $\varepsilon \in K_+^*$, existe $N'' \in \mathbb{N}$ tal que se $m, n > N''$ se tem

$$|x_n - x_m| < \varepsilon c^2.$$

Tome $N = \max\{N', N''\}$, logo para $m, n > N$ se tem

$$|y_n - y_m| = \left| \frac{1}{x_n} - \frac{1}{x_m} \right| = \left| \frac{x_m - x_n}{x_n x_m} \right| \leq \frac{|x_m - x_n|}{c^2} < \frac{\varepsilon c^2}{c^2} = \varepsilon.$$

Portanto y é fundamental em K . \square

O corpo $S_f(K)/S_0(K)$ será denotado por \hat{K} e chamado o complemento de K . É claro que

$$\begin{array}{ccc} S_c(K) & \longrightarrow & \hat{K} \\ x & \longmapsto & \bar{x} \end{array}$$

é um homomorfismo de anéis cujo núcleo é $S_0(K)$, logo existe um homomorfismo injetor

$$K \simeq S_c(K)/S_0(K) \longrightarrow \hat{K}$$

que nos permite enxergar \hat{K} como uma extensão do corpo K . O complemento de \mathbb{Q} será denotado por \mathbb{R} e chamado de *corpo dos números reais*. Na próxima seção estudaremos as propriedades do corpo \hat{K} .

Problemas

3.1 Mostre que toda subseqüência de uma seqüência fundamental é uma seqüência fundamental.

3.2 Mostre que se uma seqüência fundamental tem uma subseqüência convergente, então a seqüência é convergente e tem o mesmo limite que o da subseqüência.

3.3 Mostre que num corpo arquimediano toda seqüência monótona decrescente e limitada inferiormente é fundamental.

Sugestão: Se x possui as propriedades acima, então aplique a Proposição 9 a $-x$.

3.4 Seja K um corpo ordenado e seja $a \in K$ com $a \geq 0$. Defina a seqüência x recorrentemente por

$$x_1 = 1 , \quad x_{n+1} = \frac{2ax_n}{a + x_n^2} , \quad \forall n \in \mathbb{N}.$$

Mostre que x é monótona crescente e limitada superiormente. Conclua que se K é arquimediano, então x é fundamental. Se x fosse convergente qual seria o seu limite?

3.5 Determine os elementos invertíveis de $S(K)$, $S_f(K)$ e de $S_c(K)$. Mostre que se $x \in S_c(K) \setminus S_0(K)$, então existe algum $r \in \mathbb{N}$ tal que $y = x \circ \tau_r$ é invertível e

$$\lim y^{-1} = (\lim x)^{-1}.$$

4. Ordenação do Completamento

Nesta seção estendemos a ordenação de K para \hat{K} e estudamos as suas propriedades.

Proposição 15. *Seja $x = (x_n) \in S_f(K)$. Então uma e somente uma das seguintes condições é satisfeita*

- (i) $x \in S_0(K)$;
- (ii) Existem $c \in K_+^*$ e $N \in \mathbb{N}$ tais que $x_n \geq c$, $\forall n > N$
- (iii) Existem $c \in K_+^*$ e $N \in \mathbb{N}$ tais que $x_n \leq -c$, $\forall n > N$.

Demonstração: É claro que as condições acima são mutuamente exclusivas. Suponha que $x \notin S_0(K)$, logo pela Proposição 14 existem $c \in K_+^*$ e $N \in \mathbb{N}$ tais que $|x_n| > c$, $\forall n > N$.

Assim, se $n > N$, temos que $x_n \geq c$, se $x_n > 0$ e $-x_n \geq c$, se $x_n < 0$. Vamos provar que o sinal de x_n é fixo para n grande. Suponha que para todo $N \in \mathbb{N}$, tenhamos n e m inteiros com $m, n > N$ tais que

$$x_n \geq c \quad \text{e} \quad -x_m \geq c.$$

Logo

$$x_n - x_m \geq 2c > 0,$$

contradizendo o fato de x ser fundamental. \square

Definimos $S_f(K)^+$ como sendo o subconjunto de $S_f(K)$ união de $S_0(K)$ com o conjunto

$$\{x \in S_f(K) \mid \exists c \in K_+^*, \exists N \in \mathbb{N} \text{ com } x_n \geq c, \forall n > N\}.$$

Lema 3. Valem as seguintes afirmações

- (i) Se $x \in S_f(K)^+$ e $-x \in S_f(K)^+$, então $x \in S_0(K)$;
- (ii) Se $x, y \in S_f(K)^+$, então $x + y, x \cdot y \in S_f(K)^+$.

Demonstração: É uma simples verificação que é deixada a cargo do leitor. \square

Definimos a seguinte relação em \hat{K} ,

$$\bar{x} \leq \bar{y} \iff y - x \in S_f(K)^+.$$

Como a definição acima diz respeito a classes em \hat{K} , porém é dada em termos de representantes destas classes, devemos verificar que ela é bem posta. Para isto, devemos mostrar que se $x' - x, y' - y \in S_0(K)$ e se $y - x \in S_f(K)^+$, então $y' - x' \in S_f(K)^+$. De fato, se $x' = x + x''$ e $y' = y + y''$ com $x'', y'' \in S_0(K)$ e $y - x \in S_f(K)^+$, então $y'' - x'' \in S_0(K) \subset S_f(K)^+$ e portanto pelo Lema 3, (ii), temos que

$$y' - x' = y - x + (y'' - x'') \in S_f(K)^+.$$

A relação acima definida é uma relação de ordem em \hat{K} conforme verificaremos abaixo.

Teorema 3. $(\hat{K}, +, \cdot, \leq)$ com a relação \leq acima definida é uma extensão ordenada do corpo ordenado $(K, +, \cdot, \leq)$.

Demonstração: Já vimos no Teorema 2 que $(\hat{K}, +, \cdot)$ é uma extensão de $(K, +, \cdot)$. Vamos mostrar agora que $(\hat{K}, +, \cdot, \leq)$ é um anel ordenado.

Reflexividade. Para todo $\bar{x} \in \hat{K}$, temos que $\bar{x} \leq \bar{x}$ pois

$$x - x = 0 \in S_0(K) \subset S_f(K)^+$$

Antisimetria. Se $\bar{x} \leq \bar{y}$ e $\bar{y} \leq \bar{x}$, então $\bar{x} = \bar{y}$. De fato, temos que $y - x \in S_f(K)^+$ e $-(y - x) \in S_f(K)^+$, logo pelo Lema 3, (i) temos que $y - x \in S_0(K)$ e portanto $\bar{x} = \bar{y}$.

Transitividade. Se $\bar{x} \leq \bar{y}$ e $\bar{y} \leq \bar{z}$, então $\bar{x} \leq \bar{z}$. De fato, como $y - x \in S_f(K)^+$ e $z - y \in S_f(K)^+$, segue do Lema 3, (ii), que

$$z - x = (y - x) + (z - y) \in S_f(K)^+,$$

e consequentemente $\bar{x} \leq \bar{z}$.

Totalidade. Dados $\bar{x}, \bar{y} \in \hat{K}$, então $\bar{x} \leq \bar{y}$ ou $\bar{y} \leq \bar{x}$. De fato, dados $x, y \in S_f(K)$, então pela Proposição 15 temos que $y - x \in S_f(K)^+$ ou $-(y - x) \in S_f(K)^+$, daí segue que $\bar{x} \leq \bar{y}$ ou $\bar{y} \leq \bar{x}$.

Compatibilidade com a Adição. Sejam $\bar{x}, \bar{y}, \bar{z} \in \hat{K}$. Se $\bar{x} \leq \bar{y}$, então segue imediatamente da definição que $\bar{x} + \bar{z} \leq \bar{y} + \bar{z}$.

Compatibilidade com a Multiplicação Sejam $\bar{x}, \bar{y}, \bar{z} \in \hat{K}$ com $\bar{z} \geq 0$ e $\bar{x} \leq \bar{y}$, então $\bar{x} \cdot \bar{z} \leq \bar{y} \cdot \bar{z}$. De fato, se $y - x \in S_f(K)^+$ e $z \in S_f(K)^+$, pelo Lema 3, (ii), segue que $(y - x)z \in S_f(K)^+$ e portanto $\bar{x} \cdot \bar{z} \leq \bar{y} \cdot \bar{z}$.

Só falta agora mostrar que a relação \leq de \hat{K} é uma extensão a \hat{K} da relação \leq de K . Isto se vê como segue. Suponha $a, b \in K$ com $a \leq b$. Identificando a e b com as seqüências constantes $a_n = a$ e $b_n = b$, $\forall n \in \mathbb{N}$, é claro que $b - a \in S_f(K)^+$ e consequentemente, $\bar{a} \leq \bar{b}$. \square

Proposição 16. *Se K é arquimediano, então \hat{K} é arquimediano.*

Demonstração: Seja $\bar{x} \in \hat{K}$. Como $x \in S_f(K)$, segue que x é limitada (Proposição 11), logo temos para algum $r \in K_+^*$, que

$$x_n \leq r , \quad \forall n \in \mathbb{N}.$$

Como K é arquimediano, segue que existe $m \in \mathbb{N}$ tal que $m1 \geq r + 1$. Temos então que

$$m1 - x_n \geq 1 , \quad \forall n \in \mathbb{N}.$$

Segue que

$$m1 - x \in S_f(K)^+,$$

logo $\bar{x} \leq m\bar{1}$. \square

Lema 4. *Sejam $x, y \in S_f(K)$. Se existir $N \in \mathbb{N}$ tal que*

$$x_n \geq y_n , \quad \forall n > N,$$

então $\bar{x} \geq \bar{y}$.

Demonstração: A condição $x_n \geq y_n$, $\forall n > N$, em virtude da Proposição 15, implica que $x - y \in S_f(K)^+$, logo $\bar{x} \leq \bar{y}$. \square

Lema 5. Seja K um corpo arquimédiano e seja $\mathbf{x} = (x_n) \in S_f(K)$. Considerando (\bar{x}_n) como seqüência em \hat{K} , temos que

$$\lim_{n \rightarrow \infty} \bar{x}_n = \bar{x}.$$

Demonstração: Pela Proposição 16 temos que \hat{K} é arquimédiano e portanto dado $\varepsilon \in \hat{K}_+^*$, pela Proposição 7, existe $\varepsilon' \in K_0 \subset K$ tal que $0 < \bar{\varepsilon}' < \varepsilon$. Para este ε' , dado que \mathbf{x} é fundamental em K , existe $N \in \mathbb{N}$ tal que

$$|x_n - x_m| < \varepsilon' , \quad \forall m, n > N.$$

Para cada $m > N$ fixo, temos que

$$x_m - \varepsilon' < x_n < x_m + \varepsilon' , \quad \forall n > N$$

logo pelo Lema 4

$$\bar{x}_m - \bar{\varepsilon}' \leq \bar{x} \leq \bar{x}_m + \bar{\varepsilon}'$$

e consequentemente, para todo $m > N$, temos que

$$|\bar{x}_m - \bar{x}| \leq \bar{\varepsilon}' < \varepsilon$$

e portanto

$$\lim_{m \rightarrow \infty} \bar{x}_m = \bar{x}. \quad \square$$

O resultado seguinte nos fornece uma propriedade fundamental do completamento \hat{K} de um corpo arquimédiano K .

Teorema 4. Seja K um corpo arquimédiano e seja \hat{K} o seu complemento. Temos que toda seqüência fundamental em \hat{K} é convergente em \hat{K} , isto é,

$$S_f(\hat{K}) = S_c(\hat{K}).$$

Demonstração: Seja $X = (X_n) \in S_f(\hat{K})$. Para cada $n \in \mathbb{N}$ é possível, em vista da Proposição 7, encontrar $a_n \in K_0$ tal que

$$X_n - \frac{1}{n!} \leq \bar{a}_n \leq X_n + \frac{1}{n!},$$

isto é, tal que

$$|X_n - \bar{a}_n| \leq \frac{1}{n!}.$$

Como X é fundamental, dado $\varepsilon \in \hat{K}_+^*$, existe N , tal que

$$|X_n - X_m| \leq \frac{\varepsilon}{3}, \quad \forall m, n > N.$$

Seja $N_1 \in \mathbb{N}$ tal que $N_1 \geq N$ e $\overline{N_1 1} > \frac{3}{\varepsilon}$. Temos então para todo $m, n \geq N_1$ que

$$\begin{aligned} |\bar{a}_n - \bar{a}_m| &\leq |\bar{a}_n - X_n + X_n - X_m + X_m - \bar{a}_m| \\ &\leq |\bar{a}_n - X_n| + |X_n - X_m| + |X_m - \bar{a}_m| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon. \end{aligned}$$

Isto prova que $a = (a_n) \in S(K_0)$ é fundamental, logo pelo Lema 5 temos que

$$\lim_{n \rightarrow \infty} \bar{a}_n = \bar{a}.$$

Temos então que dado $\varepsilon \in \hat{K}_+^*$, existe $N \in \mathbb{N}$ tal que

$$|X_n - \bar{a}_n| < \frac{\varepsilon}{2} \quad \text{e} \quad |\bar{a}_n - \bar{a}| < \frac{\varepsilon}{2}, \quad \forall n > N.$$

Logo para $n > N$, temos que

$$|X_n - \bar{a}| \leq |X_n - \bar{a}_n| + |\bar{a}_n - \bar{a}| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

o que prova que

$$\lim X = \bar{a},$$

e portanto X é convergente. \square

Um corpo L tal que $S_f(L) = S_c(L)$ será dito *completo*. Portanto o Teorema 4 nos garante que o completamento \hat{K} de um corpo arquimediano K é completo.

Em particular, temos que o complemento \mathbb{R} de \mathbb{Q} é um corpo arquimediano completo. Estas três últimas propriedades caracterizam totalmente o corpo dos números reais como veremos mais adiante. A vantagem de \mathbb{R} sobre \mathbb{Q} é que em \mathbb{R} existe um número cujo quadrado é 2, isto é, existe $\sqrt{2}$. De fato, a seqüência r que introduzimos na seção 3 é fundamental em \mathbb{R} e portanto converge em \mathbb{R} a um número α tal que $\alpha^2 = 2$. Isto é apenas uma pequena indicação de que \mathbb{R} tem muitas propriedades não compartilhadas por \mathbb{Q} .

Note que em decorrência do Problema 3.4 temos que num corpo arquimediano completo K , todo elemento $a \geq 0$ possui raiz quadrada, isto é, existe $b \in K$ tal que $b^2 = a$.

Teorema 5. *Seja K um corpo arquimediano completo. Então existe um único homomorfismo de anéis de \mathbb{R} em K . Além disso, este homomorfismo é um isomorfismo de anéis ordenados.*

Demonstração: Vamos inicialmente mostrar que sendo \mathbb{R} completo, qualquer homomorfismo de \mathbb{R} num corpo ordenado é ordenado. De fato, se $a, b \in \mathbb{R}$ com $a \leq b$, segue que $b - a \geq 0$, logo existe $c \in \mathbb{R}$ tal que $c^2 = b - a$. Temos então que

$$0 \leq [f(c)]^2 = f(c^2) = f(b - a) = f(b) - f(a),$$

logo $f(a) \leq f(b)$.

Vamos agora mostrar a unicidade. Sejam f e g dois homomorfismos de \mathbb{R} num corpo arquimediano L . Considere o conjunto

$$M = \{x \in \mathbb{R} \mid f(x) = g(x)\}.$$

É fácil verificar que M é um subcorpo de \mathbb{R} . Queremos provar que $M = \mathbb{R}$. Suponha por absurdo que $M \neq \mathbb{R}$. Seja $a \in \mathbb{R} \setminus M$ que podemos supor positivo. Suponha que $f(a) < g(a)$. Temos pela Proposição 7 que existe $r \in L_0$ tal que

$$f(a) < r < g(a). \quad (1)$$

Como $L_0 = \tilde{\rho}(\mathbb{Q})$ e $\tilde{\rho}$ é o único homomorfismo de \mathbb{Q} em L segue que $f|_{\mathbb{Q}} = g|_{\mathbb{Q}} = \tilde{\rho}$ e portanto existe $s \in \mathbb{Q}$ tal que $r = \tilde{\rho}(s) = f(s) = g(s)$. Vamos mostrar que isto gera uma contradição. Temos duas possibilidades $a \leq s$ ou $s \leq a$.

Se $a \leq s$, segue que $g(a) \leq g(s) = r$, contradição com (1).

Se $s \leq a$, segue que $r = f(s) \leq f(a)$, contradição com (1).

Agora vamos mostrar a existência de um homomorfismo de \mathbb{R} em K . Considere a seguinte lei

$$\begin{aligned} \psi: S_f(\mathbb{Q}) &\longrightarrow K \\ (x_n) &\longmapsto \lim_{n \rightarrow \infty} \tilde{\rho}(x_n) \end{aligned}$$

Vamos mostrar que a lei acima está bem definida, isto é, que o limite da direita existe. Como K é completo bastará mostrar que $(\tilde{\rho}(x_n))$ é uma seqüência fundamental. De fato, dado $\varepsilon \in K_+^*$, como K é arquimediano, pela Proposição 7, temos que existe $v \in \mathbb{Q}_+^*$ tal que

$$0 < \tilde{\rho}(v) < \varepsilon.$$

Como (x_n) é fundamental, existe $N \in \mathbb{N}$ tal que

$$|x_n - x_m| < v, \quad \forall n, m > N.$$

Pelo fato de $\tilde{\rho}$ ser um homomorfismo ordenado, temos que

$$|\tilde{\rho}(x_n) - \tilde{\rho}(x_m)| < \tilde{\rho}(v) < \varepsilon, \quad \forall n, m > N.$$

Logo $(\tilde{\rho}(x_n))$ é fundamental em K . É fácil verificar que ψ é um homomorfismo de anéis. Este homomorfismo é sobrejetor pois, dado $\alpha \in K$, existe pela Proposição 7 uma seqüência $(s_n) \in S(\mathbb{Q})$ tal que $\lim_{n \rightarrow \infty} \tilde{\rho}(s_n) = \alpha$. Basta agora provar que $(s_n) \in S_f(\mathbb{Q})$. Este fato decorre de termos que $\tilde{\rho}(s_n) \in S_f(K_0)$ e $\tilde{\rho}: \mathbb{Q} \rightarrow K_0$ é um isomorfismo ordenado de anéis.

É claro também que o núcleo de ψ é $S_0(\mathbb{Q})$. Pelo Teorema do isomorfismo, temos um isomorfismo

$$\mathbb{R} = S_f(\mathbb{Q})/S_0(\mathbb{Q}) \simeq K. \quad \square$$

Corolário 1. *Todo corpo arquimédiano completo K é ordenadamente isomorfo ao corpo dos números reais, através de um único isomorfismo $\hat{\rho}: \mathbb{R} \rightarrow K$.*

Corolário 2. *O homomorfismo identidade é o único homomorfismo de anéis de \mathbb{R} em \mathbb{R} .*

Corolário 3. *Todo corpo arquimédiano é ordenadamente isomorfo a um subcorpo de \mathbb{R} .*

Demonstração: Seja K um corpo arquimédiano. Então K é ordenadamente isomorfo a um subcorpo de \hat{K} que pelo Corolário 1 é ordenadamente isomorfo a \mathbb{R} . \square

5. Relação com a Análise

Usualmente o ponto de partida da Análise Matemática é de admitir o Princípio do Supremo em \mathbb{R} (veja por exemplo o livro Análise Real I de Elon Lages Lima nesta mesma coleção). Para enunciarmos o princípio necessitaremos das seguintes definições.

Sejam K um corpo ordenado e A um subconjunto de K .

Um elemento $b \in K$ será chamado de *supremo* de A se

- (i) Para todo $x \in A$, tem-se que $x \leq b$;
- (ii) Para todo $\varepsilon \in K_+^*$, existe $x \in A$ tal que $b - \varepsilon < x \leq b$.

O supremo de um conjunto A , se existir, é único. De fato, sejam b e b' dois supremos de A . Se $b \neq b'$, digamos que $b < b'$, então por (ii) acima, temos que existe $x \in A$ tal que

$$b = b' - (b' - b) < x,$$

o que é um absurdo pois por (i) temos que $x \leq b$, $\forall x \in A$.

O supremo de A , caso exista, será denotado por $\text{Sup } A$.

O conjunto A será dito *limitado superiormente*, se existir $L \in K$ tal que $x \leq L$, $\forall x \in A$.

Teorema 6 (Princípio do Supremo). *Todo subconjunto de \mathbb{R} não vazio e limitado superiormente admite um supremo.*

Demonstração: Seja A um subconjunto de \mathbb{R} não vazio e limitado superiormente. Para cada $n \in \mathbb{N}$ defina

$$S_n = \{x \in \mathbb{Z} \mid \frac{x}{n} \geq a, \forall a \in A\}.$$

Pela propriedade arquimédiana de \mathbb{R} , temos que S_n é não vazio. É claro também que S_n é limitado inferiormente. Logo pelo Princípio da Boa Ordenação S_n tem um menor elemento que denotaremos por x_n . Pela definição de x_n temos que existe $a_n \in A$ tal que

$$\frac{x_n}{n} - \frac{1}{n} = \frac{x_n - 1}{n} < a_n \leq \frac{x_n}{n}. \quad (1)$$

Considere a seqüência definida por

$$z_n = \frac{x_n}{n}.$$

Sejam m e n inteiros positivos. Suponhamos que $\frac{x_n}{n} \geq \frac{x_m}{m}$ (o outro caso é análogo). Temos de (1) que

$$\frac{x_n}{n} - \frac{1}{n} < a_n \leq \frac{x_m}{m} \leq \frac{x_n}{n} < \frac{x_n}{n} + \frac{1}{n},$$

logo

$$|z_n - a_n| < \frac{1}{n} \quad (2)$$

e

$$|z_m - z_n| < \frac{1}{n} \quad (3)$$

De (3) segue facilmente que (z_n) é uma seqüência fundamental.

Como \mathbb{R} é completo, segue que (z_n) é convergente. Digamos que

$$\lim_{n \rightarrow \infty} z_n = z.$$

Como $z_n \geq a$, $\forall a \in A$, segue que (veja Problema 1.6),

$$z = \lim_{n \rightarrow \infty} z_n \geq a, \quad \forall a \in A.$$

Vamos mostrar que $z = \text{Sup } A$. Seja $\varepsilon \in \mathbb{R}_+^*$ e tome $N' = \frac{2}{\varepsilon}$, logo de (2) temos que se $n > N'$, então

$$|z_n - a_n| < \frac{\varepsilon}{2}.$$

Por outro lado, existe N'' tal que se $n > N''$, então

$$|z - z_n| < \frac{\varepsilon}{2}.$$

Tomando $N = \max\{N', N''\}$ temos que se $n > N$, então

$$z - a_n = |z - a_n| \leq |z - z_n| + |z_n - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto existe $a_n \in A$ tal que $z - \varepsilon < a_n$, o que prova que $z = \text{Sup } A$.

□

O próximo resultado nos garantirá a existência em \mathbb{R} da raiz n -ésima de um número real positivo qualquer, para todo $n \in \mathbb{N}$.

Teorema 7. *Dados $a \in \mathbb{R}^+$ e $n \in \mathbb{N}$, existe $b \in \mathbb{R}$ tal que $b^n = a$.*

Demonstração: Considere o conjunto

$$A = \{x \in \mathbb{R} \mid x^n \leq a\}.$$

O conjunto A é não vazio e limitado superiormente, logo pelo Teorema 6, admite um supremo. Ponhamos $b = \text{Sup } A$. Vamos mostrar que $b^n = a$.

Dado $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1$, é fácil verificar usando o binômio de Newton que existe um número real positivo r tal que

$$(1 + \varepsilon)^n < 1 + r\varepsilon.$$

Suponha que $b^n < a$. Vamos mostrar que isto leva a uma contradição. Escolha $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1$ e $\varepsilon < \frac{1}{r} \left(\frac{a}{b^n} - 1 \right)$, logo

$$b^n(1 + \varepsilon)^n < b^n(1 + r\varepsilon) < a,$$

absurdo pois $[b(1 + \varepsilon)]^n < a$ implica que $b(1 + \varepsilon) \in A$, contradizendo o fato de que $b = \text{Sup } A$.

Suponha que $b^n > a$. Vamos mostrar que isto também leva a uma contradição. Para todo $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1$ e $\varepsilon < \frac{1}{r} \left(\frac{b^n}{a} - 1 \right)$, tem-se que

$$\frac{b^n}{(1 + \varepsilon)^n} > \frac{b^n}{1 + r\varepsilon} > a,$$

o que é absurdo pois sendo $b = \text{Sup } A$, dado $\varepsilon' \in \mathbb{R}_+^*$ deve existir $x \in A$ tal que $b - \varepsilon' < x \leq b$. Isto não ocorre pois tomando

$$\varepsilon' = \frac{b\varepsilon''}{1 + \varepsilon''}$$

onde

$$\varepsilon'' = \min \left\{ 1, \frac{1}{r} \left(\frac{b^n}{a} - 1 \right) \right\},$$

tem-se para todo x tal que $b - \varepsilon' < x \leq b$, existe ε tal que

$$x = \frac{b}{1 + \varepsilon} \quad \text{e} \quad x^n = \frac{b^n}{(1 + \varepsilon)^n} > a,$$

isto é, $x \notin A$. □

O número real não negativo b tal que $b^n = a$ é denotado por $\sqrt[n]{a}$. Sejam $a, c \in \mathbb{R}^+$ e sejam b e d tais que $b^n = a$ e $d^n = c$, logo

$$a \cdot c = b^n \cdot d^n = (b \cdot d)^n$$

e consequentemente

$$\sqrt[n]{a \cdot c} = b \cdot d = \sqrt[n]{a} \cdot \sqrt[n]{c},$$

ou seja

$$\sqrt[n]{a \cdot c} = \sqrt[n]{a} \cdot \sqrt[n]{c}.$$

Os Números Complexos

O corpo dos números reais foi criado com o objetivo de completar o corpo dos números racionais de modo que equações do tipo $x^2 = 2$ tivessem soluções. Com isto muitas lacunas dos racionais, mas não todas, foram preenchidas. Por exemplo, equações como $x^2 = -1$ continuam sem solução em \mathbb{R} . A fim de sanar esta lacuna é que se resolveu após muitas vacilações ampliar o corpo dos números reais criando o corpo dos números complexos \mathbb{C} . É curioso observar que historicamente a construção formal dos números complexos precedeu a dos números reais.

Desde a antiguidade os matemáticos se depararam com o problema de extrair raízes quadradas de números negativos o que era considerado impossível. Cardan^{em} 1545 foi o primeiro matemático que efetuou operações com os números complexos apesar de não compreendê-los. Por exemplo, na procura de dois números cuja soma é 10 e cujo produto é 40, ele encontrou os “números” $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$, que somados e multiplicados nos dão respectivamente 10 e 40.

O primeiro matemático a olhar os números complexos com mais naturalidade foi Wallis que em 1675 teve a idéia de representá-los geometricamente, não indo porém além disso. Sustentava ele que se as raízes quadradas de números negativos fossem consideradas como absurdas, absurdo também seria aceitar as quantidades negativas que na época eram totalmente aceitas. A sua argumentação era a seguinte, não há razão para aceitar comprimentos negativos e rejeitar áreas negativas !

Em seguida, foi Leibniz quem considerou os números complexos

mostrando em 1676 que

$$\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}} = \sqrt{6}$$

e em 1702 que

$$\begin{aligned} x^4 + a^4 &= \left(x + a\sqrt{-\sqrt{-1}} \right) \left(x - a\sqrt{-\sqrt{-1}} \right) \\ &\quad \left(x + a\sqrt{\sqrt{-1}} \right) \left(x - a\sqrt{\sqrt{-1}} \right). \end{aligned}$$

O passo seguinte foi dado no século 18 por de Moivre e Euler que relacionaram, por meio dos números complexos, a função exponencial com as funções trigonométricas.

A teoria se consolidou com a representação geométrica das operações de adição e multiplicação de números complexos elaborada no final do século 18 por Wessel, Argand e Gauss, culminando com o chamado Teorema Fundamental da Álgebra demonstrado por Gauss e que afirma que toda equação algébrica definida sobre \mathbb{C} admite pelo menos uma raiz.

Os fatos que utilizaremos aqui e que não foram abordados no texto são a existência e propriedades básicas das funções trigonométricas seno e cosseno.

1. O Corpo dos Números Complexos

Consideremos o conjunto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ dos pares de números reais (x, y) e nele definamos as seguintes operações de adição e multiplicação:

$$\begin{aligned} (a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + b_1 \cdot a_2) \end{aligned}$$

A adição acima é simplesmente a adição de vetores em \mathbb{R}^2 enquanto que a multiplicação tem uma interpretação geométrica mais elaborada que veremos na seção 3. O conjunto \mathbb{R}^2 com as operações acima definidas será denotado por \mathbb{C} .

Teorema 1. \mathbb{C} é um corpo.

Demonstração: A associatividade e a comutatividade da adição são óbvias. O elemento zero é $(0,0)$ pois para todo $(a, b) \in \mathbb{C}$, temos

$$(a, b) + (0, 0) = (a, b).$$

O simétrico de (a, b) é $(-a, -b)$ pois

$$(a, b) + (-a, -b) = (0, 0).$$

A associatividade, comutatividade da multiplicação e a distributividade da multiplicação com relação à adição são de verificação direta. A unidade da multiplicação é $(1,0)$ pois para todo $(a, b) \in \mathbb{C}$,

$$(a, b) \cdot (1, 0) = (a, b).$$

O inverso de $(a, b) \neq (0, 0)$ é $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ pois

$$(a, b) \cdot \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = (1, 0) \quad \square$$

Chamaremos \mathbb{C} de *corpo dos números complexos*, e os seus elementos de *números complexos*.

Seja $(a, b) \in \mathbb{C}$, podemos escrever

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1). \quad (1)$$

Portanto, todo número complexo pode ser representado usando somente os números da forma $(x, 0)$ e o número $(0, 1)$.

Considere a função

$$\begin{aligned} \varphi: \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\longmapsto (x, 0) \end{aligned}$$

Verifica-se facilmente que φ é um homomorfismo injetor de anéis. Portanto φ permite identificar \mathbb{R} com o subcorpo $\varphi(\mathbb{R})$ de \mathbb{C} . Se por abuso de notação escrevermos x no lugar de $(x, 0)$ e i no lugar de $(0, 1)$, temos de (1) acima que

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi.$$

A forma acima é chamada *forma normal* do número complexo (a, b) . Observe que

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1,$$

portanto acabamos de construir um corpo que contém o corpo \mathbb{R} e no qual a equação $z^2 + 1 = 0$ admite uma raiz (o número i).

Na forma normal é claro que $a_1 + b_1i = a_2 + b_2i$ se e somente se $a_1 = a_2$ e $b_1 = b_2$. Além disso, opera-se usando as propriedades de corpo e a informação adicional de que $i^2 = -1$. Por exemplo,

$$(a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i,$$

$$(a_1 + b_1i) - (a_2 + b_2i) = (a_1 - a_2) + (b_1 - b_2)i$$

$$\begin{aligned} (a_1 + b_1i) \cdot (a_2 + b_2i) &= a_1a_2 + b_1a_2i + a_1b_2i + b_1b_2i^2 \\ &= (a_1a_2 - b_1b_2) + (b_1a_2 + a_1b_2)i \end{aligned}$$

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i.$$

O corpo \mathbb{C} nos forneceu uma solução para a equação $z^2 = -1$. Vamos agora mostrar que dado um número complexo qualquer $a + bi$, a equação $z^2 = a + bi$ admite solução em \mathbb{C} .

Ponha $z = x + yi$, temos então que

$$(x + yi)^2 = a + bi,$$

logo

$$x^2 - y^2 + 2xyi = a + bi,$$

portanto

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \quad (2)$$

Considere agora a seguinte identidade, válida para todos $x, y \in \mathbb{R}$,

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + 4x^2y^2 \quad (3)$$

substituindo os valores de (2) em (3), temos que

$$(x^2 + y^2)^2 = a^2 + b^2,$$

logo

$$x^2 + y^2 = \sqrt{a^2 + b^2} \quad (4)$$

Temos então de (2) e (4) o sistema,

$$\begin{cases} x^2 - y^2 = a \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases}$$

que implica

$$x = \pm \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}$$

$$y = \pm \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}$$

Ao combinarmos estes duplos sinais obtemos quatro possibilidades para as soluções. Mas de (2) temos que $2xy = b$ e portanto x e y devem ser tais que o seu produto tem o sinal de b , dando assim duas soluções para a equação $z^2 = a + bi$.

É preciso tomar cuidado com o símbolo $\sqrt{a + bi}$ pois, em contraste com o que ocorre no campo real, aqui não há nenhuma preferência em denotar $\sqrt{a + bi}$ uma ou outra solução da equação $z^2 = a + bi$. No caso real, dado $a > 0$, existem duas soluções para $x^2 = a$, uma positiva e outra negativa, sendo que a raiz positiva é simbolizada por \sqrt{a} . Já em \mathbb{C} não se adota nenhuma convenção para dar sentido ao símbolo $\sqrt{a + bi}$, a não ser quando se disser explicitamente caso por caso qual das soluções da equação $z^2 = a + bi$ se convenciona chamar de $\sqrt{a + bi}$. Por exemplo, o símbolo $\sqrt{-1}$ é reservado para o número complexo i , sendo que a outra solução da equação $z^2 = -1$ é $-i$.

Exemplos

1. Vamos resolver a equação $z^2 = -i$.

Como $a = 0$ e $b = -1$, temos que

$$x = \pm \sqrt{\frac{1}{2}} , \quad y = \pm \sqrt{\frac{1}{2}}.$$

Como $b < 0$, então as soluções da equação são

$$z_1 = \sqrt{\frac{1}{2}} - \sqrt{\frac{1}{2}}i \quad , \quad z_2 = -\sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2}}i$$

2. Resolvamos a equação $z^2 = 1 + i$.

Usando as fórmulas temos que

$$x = \pm \sqrt{\frac{\sqrt{2} + 1}{2}} \quad , \quad y = \pm \sqrt{\frac{\sqrt{2} - 1}{2}}.$$

Como $b > 0$, as soluções são

$$\begin{aligned} z_1 &= \sqrt{\frac{\sqrt{2} + 1}{2}} + \sqrt{\frac{\sqrt{2} - 1}{2}}i \\ z_2 &= -\sqrt{\frac{\sqrt{2} + 1}{2}} - \sqrt{\frac{\sqrt{2} - 1}{2}}i \end{aligned}$$

Problemas

1.1 Mostre que \mathbb{C} não é um corpo ordenado.

Sugestão: Num corpo ordenado para todo $a \neq 0$, tem-se que $a^2 > 0$. Mas, $0 < i^2 = -1 < 0$, contradição.

1.2 Coloque na forma normal os seguintes números complexos

- | | | |
|-------------------------------|---|-------------------|
| (a) $(3 + i)^2 \cdot (2 - i)$ | (b) $(4 - 3i)^3$ | (c) $\frac{1}{i}$ |
| (d) $\frac{1+i}{1-i}$ | (e) $\frac{2+i}{1-i} + \frac{3-i}{1+i}$ | |

1.3 Ache os inversos dos seguintes números complexos, na forma normal

- | | | |
|---------------|---|--------------------------------|
| (a) $2 + 3i$ | (b) $\frac{5+i}{3+i} + \frac{3+2i}{1+3i}$ | (c) $\frac{2+3i}{1+i} + 1 + i$ |
| (d) $(1+i)^3$ | | |

1.4 Mostre que

$$i^n = \begin{cases} 1 & , \text{ se } n \equiv 0 \pmod{4} \\ i & , \text{ se } n \equiv 1 \pmod{4} \\ -1 & , \text{ se } n \equiv 2 \pmod{4} \\ -i & , \text{ se } n \equiv 3 \pmod{4} \end{cases}$$

1.5 Calcule o valor de

$$3 \cdot i^{27} + 4 \cdot i^{37} - i^{30}$$

1.6 Para $n \in \mathbb{N}$, calcule o valor de $1 + i + i^2 + \dots + i^{n-1}$.

1.7 Resolva em \mathbb{C} as seguintes equações

- | | | |
|-------------------|---|---------------------------|
| (a) $z^2 = 1 - i$ | (b) $z^2 = 1 + \sqrt{3}i$ | (c) $z^2 = 1 - \sqrt{3}i$ |
| (d) $z^4 = 1 + i$ | (e) $z^4 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ | (f) $z^4 = 3 + 4i$ |

1.8 Escolhendo convenientemente $\sqrt{1 + \sqrt{3}i}$ e $\sqrt{1 - \sqrt{3}i}$, mostre que

$$\sqrt{1 + \sqrt{3}i} + \sqrt{1 - \sqrt{3}i} = \sqrt{6}$$

1.9 Sejam $a, b, c \in \mathbb{C}$ com $a \neq 0$. Mostre que as soluções da equação

$$az^2 + bz + c = 0,$$

são

$$z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{e} \quad z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

onde $\sqrt{b^2 - 4ac}$ é uma das soluções da equação $u^2 = b^2 - 4ac$.

1.10 Resolva as equações

- $iz^2 - (2 + 2i)z + 2 - i = 0;$
- $z^2 + z + 1 = 0.$

2. Conjugação e Módulo

Seja $z = a + bi \in \mathbb{C}$, com $a, b \in \mathbb{R}$. Define-se o *conjugado* de z como sendo $\bar{z} = a - bi$ e o *módulo* de z como sendo o número real $|z| = \sqrt{a^2 + b^2}$. A *parte real* e a *parte imaginária* de z são respectivamente os números reais $\operatorname{Re} z = a$ e $\operatorname{Im} z = b$.

Damos a seguir uma lista de propriedades que estes objetos possuem

Propriedades

- 1) $\bar{\bar{z}} = 0$ se e somente se $z = 0$;
- 2) $\bar{z} = z$ se e somente se $z \in \mathbb{R}$;
- 3) $\bar{\bar{z}} = z$ para todo $z \in \mathbb{C}$;
- 4) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
- 5) $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$;
- 6) Se $z_2 \neq 0$, então $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$;
- 7) Se $z \neq 0$, então $(\bar{z})^n = \overline{(z^n)}$ para todo $n \in \mathbb{Z}$;
- 8) $z \cdot \bar{z} = |z|^2$, para todo $z \in \mathbb{C}$;
- 9) $|z| = |\bar{z}| = |-z|$, para todo $z \in \mathbb{C}$;
- 10) $\operatorname{Re} z = \frac{z + \bar{z}}{2}$ e $\operatorname{Im} z = \frac{z - \bar{z}}{2i}$;
- 11) $|\operatorname{Re} z| \leq |z|$ e $|\operatorname{Im} z| \leq |\operatorname{Im} z| \leq |z|$.

Estas propriedades são fáceis de verificar. A título de ilustração provaremos a propriedade (5).

Sejam $z_1 = a_1 + b_1i$ e $z_2 = a_2 + b_2i$, a propriedade (5) é consequência das seguintes igualdades:

$$\begin{aligned}\overline{z_1 \cdot z_2} &= \overline{(a_1 + b_1i) \cdot (a_2 + b_2i)} = \overline{(a_1 a_2 - b_1 b_2) + (b_1 a_2 + a_1 b_2)i} \\ &= (a_1 a_2 - b_1 b_2) - (b_1 a_2 + a_1 b_2)i\end{aligned}$$

e

$$\bar{z}_1 \cdot \bar{z}_2 = (a_1 - b_1i) \cdot (a_2 - b_2i) = a_1 a_2 - b_1 b_2 - (b_1 a_2 + a_1 b_2)i$$

As seguintes proposições nos fornecerão alguns resultados básicos

Proposição 1. *Quaisquer que sejam $z_1, z_2 \in \mathbb{C}$, temos que*

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|$$

Demonstração: Usando as propriedades (5) e (8) acima, temos que

$$|z_1 \cdot z_2|^2 = (z_1 \cdot z_2)(\overline{z_1 \cdot z_2}) = z_1 \cdot \bar{z}_1 \cdot z_2 \cdot \bar{z}_2 = |z_1|^2 \cdot |z_2|^2 = (|z_1| \cdot |z_2|)^2.$$

Como $|z_1 \cdot z_2|$ e $|z_1| \cdot |z_2|$ são ambos números reais não negativos, extraindo a raiz quadrada de ambos os membros da igualdade $|z_1 \cdot z_2|^2 = (|z_1| \cdot |z_2|)^2$, obtemos que $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$. \square

Proposição 2. *Quaisquer que sejam $z_1, z_2 \in \mathbb{C}$, temos que*

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Demonstração: Usando as propriedades (5) e (3) acima, verifica-se que $z_1 \cdot \bar{z}_2$ e $z_2 \cdot \bar{z}_1$ são conjugados, logo pela propriedade (10) temos que $z_1 \cdot \bar{z}_2 + z_2 \cdot \bar{z}_1 = 2\operatorname{Re}(z_1 \cdot \bar{z}_2)$. Como pelas propriedade (11) e (9) e pela Proposição 1, temos que $z_1 \cdot \bar{z}_2 + z_2 \cdot \bar{z}_1 \leq 2|z_1| \cdot |z_2|$, segue pelas propriedades (8) e (4) que

$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2) \cdot (\overline{z_1 + z_2}) = z_1 \cdot \bar{z}_1 + z_1 \cdot \bar{z}_2 + z_2 \cdot \bar{z}_1 + z_2 \cdot \bar{z}_2 \\ &= |z_1|^2 + 2\operatorname{Re}(z_1 \cdot \bar{z}_2) + |z_2|^2 \leq |z_1|^2 + 2|z_1| \cdot |z_2| + |z_2|^2 \\ &= (|z_1| + |z_2|)^2. \end{aligned}$$

Extraindo a raiz quadrada dos dois extremos das desigualdade acima, obtemos o resultado. \square

Problemas

2.1 Demonstre as propriedades de (1) a (11) da conjugação e do módulo.

2.2 Ache uma condição necessária e suficiente para que valha a igualdade na Proposição 2.

2.3 Seja $S^1 = \{z \in \mathbb{C} / |z| = 1\}$. Mostre que

- (a) Se $z \in S^1$, então z é invertível e $z^{-1} = \bar{z}$;
- (b) Se $z_1, z_2 \in S^1$, então $z_1 \cdot z_2 \in S^1$;
- (c) Se $z \in S^1$, então $z^{-1} \in S^1$;
- (d) Se para algum $n \in \mathbb{Z} \setminus \{0\}$ se tem $z^n = 1$, então $z \in S^1$.

2.4 Mostre que qualquer que seja $z \in \mathbb{C}$, se tem

$$\frac{1}{\sqrt{2}}(\operatorname{Re} z + i \operatorname{Im} z) \leq |z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|.$$

3. Forma Trigonométrica dos Números Complexos

Neste seção damos a representação dos números complexos em coordenadas polares. A relação entre coordenadas cartesianas e polares resultou num dos instrumentos mais poderosos na teoria dos números complexos, sem o qual seria praticamente impossível operar com estes números, especialmente no que diz respeito à extração de raízes.

Seja $z = a + bi$ um número complexo não nulo e sejam r o módulo de z e θ o ângulo orientado (módulo 2π radianos) que o vetor (a, b) forma com o eixo $\mathbb{R} \times \{0\}$. Com estas notações temos que

$$\begin{cases} a = r \cos \theta \\ b = r \sin \theta \end{cases}$$

Podemos então escrever

$$z = r(\cos \theta + i \sin \theta),$$

a qual é chamada de *forma trigonométrica* do número complexo z . Temos portanto que $r_1(\cos \theta_1 + i \sin \theta_1) = r_2(\cos \theta_2 + i \sin \theta_2)$ se e somente se $r_1 = r_2$ e $\theta_1 = \theta_2 + 2m\pi$ para algum $m \in \mathbb{Z}$.

Exemplos

- 1) $1 = \cos 0 + i \sin 0$;
- 2) $-1 = \cos \pi + i \sin \pi$;
- 3) $i = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$;
- 4) $-i = \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}$;

$$5) \quad 1 + i = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right);$$

$$6) \quad 1 + \sqrt{3}i = 2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right)$$

Proposição 3. Sejam $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$ e $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$. Temos que

$$z_1 \cdot z_2 = r_1 \cdot r_2 [\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)]$$

Demonstração: Efetuando o produto, temos que

$$\begin{aligned} z_1 \cdot z_2 &= r_1 r_2 [(\cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2) + \\ &\quad + i(\cos \theta_1 \sin \theta_2 + \sin \theta_1 \cos \theta_2)] = \\ &= r_1 r_2 [\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)] \end{aligned}$$

□

Da Proposição 3 segue a seguinte regra:

O produto de dois números complexos tem por representação um vetor cujo módulo é o produto dos módulos destes números e cujo ângulo com o eixo $\mathbb{R} \times \{0\}$ é a soma dos ângulos (módulo 2π) que as representações destes números formam com o referido eixo.

Por exemplo, a multiplicação por i representa simplesmente uma rotação de um ângulo $\frac{\pi}{2}$ no sentido anti-horário. Mais geralmente, a multiplicação por $\cos \theta + i \sin \theta$ representa uma rotação de um ângulo θ no sentido anti-horário.

Proposição 4. Sejam $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$ e $z_2 = r_2(\cos \theta_2 + i \sin \theta_2) \neq 0$. Temos que

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} [\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)].$$

Demonstração: Observe inicialmente que

$$\bar{z}_2 = r_2(\cos \theta_2 - i \sin \theta_2) = r_2[\cos(-\theta_2) + i \sin(-\theta_2)].$$

Portanto da Proposição 3 temos que

$$\begin{aligned}\frac{z_1}{z_2} &= \frac{z_1 \cdot \bar{z}_2}{z_2 \cdot \bar{z}_2} = \frac{1}{|z_2|^2} z_1 \cdot \bar{z}_2 \\ &= \frac{1}{r_2^2} r_1 r_2 [\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)] \\ &= \frac{r_1}{r_2} [\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)].\end{aligned}$$

□

Teorema 2 (Fórmula de De Moivre). Para todo $z = r(\cos \theta + i \sin \theta) \neq 0$ e todo $n \in \mathbb{Z}$, temos que

$$[r(\cos \theta + i \sin \theta)]^n = r^n (\cos n\theta + i \sin n\theta).$$

Demonstração: Para $n = 0$, a igualdade é óbvia. Para $n \in \mathbb{N}$, isto é facilmente demonstrado por indução usando a Proposição 3. Seja agora $n < 0$. Note que se $z = \cos \alpha + i \sin \alpha$, para algum $\alpha \in \mathbb{R}$, então $z^{-1} = \bar{z} = \cos \alpha - i \sin \alpha$, pois $z \cdot \bar{z} = |z|^2 = 1$. Temos então pelo caso $(-n) \in \mathbb{N}$ que

$$\begin{aligned}[r(\cos \theta + i \sin \theta)]^n &= [(r(\cos \theta + i \sin \theta))^{-n}]^{-1} \\ [r^{-n}(\cos(-n\theta) + i \sin(-n\theta))]^{-1} &= r^n (\cos n\theta - i \sin n\theta)^{-1} \\ &= r^n (\cos n\theta + i \sin n\theta).\end{aligned} \quad \square$$

Problemas

3.1 Escreva os seguintes números complexos sob forma trigonométrica

- | | | |
|---------------------|------------|---|
| a) -6 | b) $1 - i$ | c) $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$ |
| d) $2 + 2\sqrt{3}i$ | e) $16i$ | f) $-\frac{1}{2} + \frac{\sqrt{2}}{2}i$ |

3.2 Mostre que se $\theta \neq 2\lambda\pi$ para todo $\lambda \in \mathbb{Z}$, então

$$\text{a)} \quad 1 + \cos \theta + \cdots + \cos n\theta = \frac{\cos \frac{n\theta}{2}}{\frac{\theta}{2}} \operatorname{sen} \frac{(n+1)\theta}{2};$$

$$b) \quad \sin \theta + \sin 2\theta + \cdots + \sin n\theta = \frac{\frac{\sin \frac{n\theta}{2}}{\sin \frac{\theta}{2}}}{\frac{(n+1)\theta}{2}} \cdot \frac{(n+1)\theta}{2}.$$

Sugestão: Substitua $z = \cos \theta + i \sin \theta$ na fórmula

$$1 + z + z^2 + \cdots + z^n = \frac{z^{n+1} - 1}{z - 1}.$$

3.3 Seja $n \in \mathbb{N}$. Escreva

- a) $\cos n\theta$ como polinômio de grau n em $\cos \theta$;
- b) $\sin n\theta$ como produto de $\sin \theta$ por um polinômio de grau $n-1$ em $\cos \theta$.

Sugestão: Escreva $(\cos \theta + i \sin \theta)^n$ pela fórmula de De Moivre por um lado e pelo binômio de Newton por outro.

3.4 a) Escreva $\cos 3\theta$, $\cos 4\theta$ e $\cos 5\theta$ em função de $\cos \theta$;

b) Escreva $\sin 3\theta$ e $\sin 5\theta$ em função de $\sin \theta$;

c) Escreva $\frac{\sin 4\theta}{\sin \theta}$ em função de $\cos \theta$;

d) Demonstre a identidade $\cos 5\theta + \cos 3\theta = 2 \cos \theta \cos 4\theta$.

3.5 Mostre que $\cos \frac{\pi}{9}$ satisfaz à equação $8x^3 - 6x - 1 = 0$.

Sugestão: Use o problema 3.4 (a).

3.6 Calcule $\cos 18^\circ$ e $\sin 18^\circ$.

Sugestão: Observe que $5 \times 18 = 90$ e use as expressões de $\cos 5\theta$ e $\sin 5\theta$ deduzidas no problema 3.4.

3.7 Calcule o valor de $\left(\frac{\sqrt{3}+i}{2}\right)^n$ segundo os valores de $n \in \mathbb{Z}$.

4. Raízes de Números Complexos

Sejam K um corpo e w um elemento de K . Se n é um número natural, uma *raiz n-ésima* de w é um elemento $z \in K$ tal que $z^n = w$. Dado um número complexo $w = a + bi$, queremos determinar as raízes n -

ésimas de w . Se tentarmos seguir o mesmo procedimento que no caso da extração de raízes quadradas, obtemos um sistema de equações cuja resolução é impraticável, indicando que este não é o caminho para resolver o problema. Veremos no que segue como a fórmula de De Moivre nos permitirá resolver facilmente o problema.

Teorema 3. *Sejam dados um número complexo não nulo $w = r(\cos \theta + i \operatorname{sen} \theta)$, um número natural n e seja \mathcal{R} um sistema completo de resíduos módulo n . Então w admite n raízes n -ésimas dadas por*

$$z_\lambda = \sqrt[n]{r} \left(\cos \frac{\theta + 2\lambda\pi}{n} + i \operatorname{sen} \frac{\theta + 2\lambda\pi}{n} \right) , \quad \lambda \in \mathcal{R}.$$

Demonstração: Ponhamos $z = \rho(\cos \alpha + i \operatorname{sen} \alpha)$. Queremos resolver em ρ e α a equação

$$[\rho(\cos \alpha + i \operatorname{sen} \alpha)]^n = r(\cos \theta + i \operatorname{sen} \theta).$$

Pela fórmula de De Moivre temos que

$$\rho^n (\cos n\alpha + i \operatorname{sen} n\alpha) = r(\cos \theta + i \operatorname{sen} \theta),$$

logo

$$\begin{cases} \rho^n = r \\ n\alpha = \theta + 2\lambda\pi , \quad \lambda \in \mathbb{Z}. \end{cases}$$

Temos então que

$$\begin{cases} \rho = \sqrt[n]{r} \\ \alpha = \frac{\theta + 2\lambda\pi}{n} , \quad \lambda \in \mathbb{Z}, \end{cases}$$

portanto as raízes n -ésimas de w são dadas por

$$z_\lambda = \sqrt[n]{r} \left(\cos \frac{\theta + 2\lambda\pi}{n} + i \operatorname{sen} \frac{\theta + 2\lambda\pi}{n} \right) , \quad \lambda \in \mathbb{Z}.$$

Como λ é um inteiro arbitrário, aparentemente são em número infinito as raízes n -ésimas de w . Isto não é o caso pois $z_\lambda = z_\mu$ se e somente se $\frac{1}{2\pi} \left[\frac{\theta + 2\lambda\pi}{n} - \frac{\theta + 2\mu\pi}{n} \right] \in \mathbb{Z}$, isto é equivalente a $\frac{\lambda - \mu}{n} \in \mathbb{Z}$, o que é equivalente a $\lambda \equiv \mu \pmod{n}$. Isto completa a demonstração. □

Na prática tomamos $\mathcal{R} = \{0, 1, \dots, n - 1\}$.

Exemplos

1. Resolvamos a equação $z^4 = -4$.

A forma trigonométrica de -4 é $4(\cos \pi + i \operatorname{sen} \pi)$, portanto as soluções da equação são

$$z_\lambda = \sqrt[4]{4} \left(\cos \frac{\pi + 2\lambda\pi}{4} + i \operatorname{sen} \frac{\pi + 2\lambda\pi}{4} \right) , \quad \lambda = 0, 1, 2, 3.$$

Calculando estes valores temos,

$$z_0 = \sqrt{2} \left(\cos \frac{\pi}{4} + i \operatorname{sen} \frac{\pi}{4} \right) = 1 + i$$

$$z_1 = \sqrt{2} \left(\cos \frac{3\pi}{4} + i \operatorname{sen} \frac{3\pi}{4} \right) = -1 + i$$

$$z_2 = \sqrt{2} \left(\cos \frac{5\pi}{4} + i \operatorname{sen} \frac{5\pi}{4} \right) = -1 - i$$

$$z_3 = \sqrt{2} \left(\cos \frac{7\pi}{4} + i \operatorname{sen} \frac{7\pi}{4} \right) = 1 - i$$

2. Resolvamos a equação $z^3 = i$.

Como $i = \cos \frac{\pi}{2} + i \operatorname{sen} \frac{\pi}{2}$, temos que as soluções da equação acima são

$$z_\lambda = \cos \frac{\pi/2 + 2\lambda\pi}{3} + i \operatorname{sen} \frac{\pi/2 + 2\lambda\pi}{3} , \quad \lambda = 0, 1, 2.$$

Donde

$$z_0 = \cos \frac{\pi}{6} + i \operatorname{sen} \frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{i}{2}$$

$$z_1 = \cos \frac{5\pi}{6} + i \operatorname{sen} \frac{5\pi}{6} = -\frac{\sqrt{3}}{2} + \frac{i}{2}$$

$$z_2 = \cos \frac{9\pi}{6} + i \operatorname{sen} \frac{9\pi}{6} = -i$$

3. Resolvamos a equação $z^3 = 1$.

Como $1 = \cos 0 + i \sin 0$, as soluções da equação acima são

$$z_\lambda = \cos \frac{2\lambda\pi}{3} + i \sin \frac{2\lambda\pi}{3}, \quad \lambda = 0, 1, 2.$$

Portanto

$$z_0 = \cos 0 + i \sin 0 = 1$$

$$z_1 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1 + \sqrt{3}i}{2}$$

$$z_2 = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = \frac{-1 - \sqrt{3}i}{2}$$

Problemas

4.1 Resolva as seguintes equações

- | | | |
|------------------|---|----------------|
| a) $z^3 = 1 + i$ | b) $z^3 = 1 - i$ | c) $z^4 = 16i$ |
| d) $z^4 = 1 - i$ | e) $z^4 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ | f) $z^6 = -4$ |

4.2 Compare os seguintes conjuntos, as raízes n -ésimas de i^2 e os quadrados das raízes n -ésimas de i .

5. Raízes da Unidade

Num corpo K , uma *raiz n -ésima da unidade* para $n \in \mathbb{N}$, é uma solução da equação $z^n = 1$. Se $K = \mathbb{C}$, as raízes n -ésimas da unidade são dadas por

$$\xi_\lambda = \cos \frac{2\lambda\pi}{n} + i \sin \frac{2\lambda\pi}{n}, \quad \lambda = 0, 1, \dots, n-1.$$

As raízes n -ésimas da unidade tem por representação no plano os vértices de um polígono regular de n lados inscrito no círculo unitário de centro em $z = 0$ e tendo um vértice no ponto $z = 1$. As raízes da unidade desempenham um papel importante em vários ramos da matemática e particularmente na teoria das equações algébricas.

Proposição 5. *As raízes n -ésimas da unidade em \mathbb{C} gozam das seguintes propriedades*

(i) $\xi_\lambda \cdot \xi_\mu = \xi_{\lambda+\mu}$

$$(ii) \quad \xi_\lambda^\ell = \xi_{\ell\lambda} \text{ para todo } \ell \in \mathbb{Z};$$

$$(iii) \quad \xi_\lambda^{-1} = \bar{\xi}_\lambda = \xi_{n-\lambda}$$

Demonstração: i. segue da Proposição 3, ii. segue da Fórmula de De Moivre (Teorema 1) e iii. segue do fato que $\xi_\lambda^{-1} = \xi_{-\lambda}$ (de (ii)) e do fato que $-\lambda \equiv n - \lambda \pmod{n}$. \square

Proposição 6. *Num corpo K as raízes n-ésimas de um elemento qualquer podem ser obtidas multiplicando uma raiz n-ésima qualquer fixada deste elemento pelas raízes n-ésimas da unidade.*

Demonstração: Seja $w \in K$. Se $w = 0$ é claro que a equação $z^n = w$ tem apenas a solução $z = 0$, e o resultado é banalmente verificado. Suponha que b_0 seja uma solução da equação $z^n = w$ com $w \neq 0$, logo $b_0 \neq 0$. Seja b uma solução qualquer da equação, logo $b^n = b_0^n = w$, consequentemente $(b/b_0)^n = 1$ e portanto $b/b_0 = \xi$ =raiz n-ésima da unidade, logo $b = b_0\xi$ com ξ uma raiz n-ésima da unidade. Por outro lado se ξ é uma raiz n-ésima da unidade, é fácil verificar que $b_0\xi$ é solução da equação $z^n = w$. \square

Certas raízes n-ésimas da unidade se destacam sobre as demais, vejamos um exemplo para introduzir um novo conceito.

Considere as raízes quartas da unidade

$$\xi_0 = 1, \quad \xi_1 = i, \quad \xi_2 = -1, \quad \xi_3 = -i.$$

Verifica-se facilmente que

$$\{\xi_0^n \mid n \in \mathbb{Z}\} = \{\xi_0\}$$

$$\{\xi_1^n \mid n \in \mathbb{Z}\} = \{\xi_0, \xi_1, \xi_2, \xi_3\}$$

$$\{\xi_2^n \mid n \in \mathbb{Z}\} = \{\xi_0, \xi_2\}$$

$$\{\xi_3^n \mid n \in \mathbb{Z}\} = \{\xi_0, \xi_1, \xi_2, \xi_3\}.$$

Vemos então que as raízes ξ_1 e ξ_3 tem a propriedade de gerar por potenciação todas as raízes quartas da unidade. A seguinte proposição caracterizará as raízes n-ésimas da unidade que possuem tal propriedade.

Proposição 7. *Seja $\xi_\lambda = \cos \frac{2\lambda\pi}{n} + i \sin \frac{2\lambda\pi}{n}$ com $\lambda \in \mathbb{Z}$ e $n > 1$, uma raiz n-ésima da unidade. As seguintes condições são equivalentes*

- (i) $\xi_\lambda^0, \xi_\lambda^1, \dots, \xi_\lambda^{n-1}$ são todas as raízes n -ésimas da unidade;
- (ii) $\xi_\lambda^m \neq 1$ para todo m tal que $0 < m < n$;
- (iii) $(n, \lambda) = 1$.

Demonstração:

(i) \Rightarrow (ii): Suponha por absurdo que $\xi_\lambda^m = 1$ para algum m tal que $0 < m < n$, como $\xi_\lambda^0 = 1$, os números $\xi_\lambda^0, \xi_\lambda^1, \dots, \xi_\lambda^{n-1}$ não são todos distintos e portanto não podem representar todas as raízes n -ésimas da unidade.

(ii) \Rightarrow (iii): Suponha por absurdo que $d = (n, \lambda) \neq 1$. Temos então que $\lambda = ld$ para algum $l \in \mathbb{Z}$ e $n = m \cdot d$ para algum $m \in \mathbb{Z}$ tal que $0 < m < n$. Segue então pela Proposição 5, que

$$\xi_\lambda^m = \xi_{\ell d}^m = \xi_{m \ell d} = \xi_{n \ell} = \xi_\ell^n = 1,$$

contradição.

(iii) \Rightarrow (i): Se $(n, \lambda) = 1$, então $\{0, \lambda, 2\lambda, \dots, (n-1)\lambda\}$ é um sistema completo de resíduos módulo n (veja Problema 2.1 (b), Capítulo 6), logo

$$\{\xi_\lambda^0, \xi_\lambda^1, \xi_\lambda^2, \dots, \xi_\lambda^{n-1}\} = \{\xi_0, \xi_\lambda, \xi_{2\lambda}, \dots, \xi_{(n-1)\lambda}\}$$

é o conjunto de todas as raízes n -ésimas da unidade. □

Uma raiz n -ésima da unidade que goza das propriedades equivalentes da proposição é chamada *raiz n -ésima primitiva da unidade*.

Corolário. O número de raízes n -ésimas primitivas da unidade é $\Phi(n)$.

Demonstração: Isto segue da propriedade (iii) da proposição e recordando que $\Phi(n)$ representa o número de inteiros λ tais que $0 < \lambda < n$ e $(n, \lambda) = 1$. □

Proposição 8. Seja K um corpo. Um elemento $\xi \in K$ é simultaneamente raiz n -ésima e raiz m -ésima da unidade se e somente se ξ é raiz d -ésima da unidade, onde $d = (m, n)$.

Demonstração: Suponha que $\xi^n = \xi^m = 1$. Se $d = (m, n)$, então

existem $r, s \in \mathbb{Z}$ tais que $d = rm + sn$, logo

$$\xi^d = \xi^{rm+sn} = (\xi^m)^r(\xi^n)^s = 1.$$

Reciprocamente, suponha que $\xi^d = 1$. Como $n = td$ e $m = \ell d$ para t e ℓ em \mathbb{Z} , segue que

$$\xi^n = \xi^{td} = (\xi^d)^t = 1$$

e que

$$\xi^m = \xi^{\ell d} = (\xi^d)^\ell = 1. \quad \square$$

Corolário. Se $(m, n) = 1$, então 1 é a única raiz simultaneamente n -ésima e m -ésima da unidade.

Por exemplo, as raízes simultaneamente 28-ésimas e 32-ésimas da unidade são as raízes quartas da unidade, pois $(28, 32) = 4$. Portanto estas são 1, i , -1 e $-i$.

Proposição 9. Suponha que $\xi, \eta \in \mathbb{C}$ são respectivamente raízes p -ésimas e q -ésimas primitivas da unidade. Se $(p, q) = 1$, então $\xi\eta$ é raiz pq -ésima primitiva da unidade.

Demonstração: Inicialmente observe que $\xi\eta$ é raiz pq -ésima da unidade pois

$$(\xi\eta)^{p \cdot q} = (\xi^p)^q(\eta^q)^p = 1.$$

Suponha que $\xi\eta$ não seja raiz pq -ésima primitiva da unidade. Existe então $m \in \mathbb{N}$ tal que $m < pq$ e $(\xi\eta)^m = 1$. Pela divisão euclidiana em \mathbb{Z} , existem $n_1, n_2, r_1, r_2 \in \mathbb{Z}$ tais que $m = pn_1 + r_1$ e $m = qn_2 + r_2$ com $0 \leq r_1 < p$ e $0 \leq r_2 < q$. Logo

$$1 = (\xi\eta)^m = \xi^{pn_1+r_1}\eta^{qn_2+r_2} = (\xi^p)^{n_1}(\eta^q)^{n_2}\xi^{r_1}\eta^{r_2} = \xi^{r_1}\eta^{r_2}.$$

Temos então que ξ^{r_1} é o inverso da raiz q -ésima da unidade η^{r_2} e portanto também raiz q -ésima da unidade. Segue então que ξ^{r_1} é simultaneamente raiz p -ésima e raiz q -ésima da unidade e consequentemente pelo Corolário da Proposição 8, temos que $\xi^{r_1} = 1$. Como ξ é raiz p -ésima primitiva da unidade e $0 \leq r_1 < p$, segue que $r_1 = 0$.

Um raciocínio totalmente análogo implica que $r_2 = 0$. Consequentemente temos que $p \mid m$ e $q \mid m$ e como $(p, q) = 1$, temos que $pq \mid m$. Isto contradiz o fato que $0 < m < pq$. \square

Corolário. Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ um inteiro maior do que ou igual a 2 decomposto em fatores primos. Sejam η_i com $i = 1, \dots, r$ respectivamente raízes $p_i^{\alpha_i}$ -ésimas primitivas da unidade. Então $\eta = \eta_1 \cdots \eta_r$ é raiz n -ésima primitiva da unidade.

Exemplo: Considere a raiz quarta primitiva da unidade

$$\xi = \cos \frac{2\pi}{4} + i \sin \frac{2\pi}{4},$$

e a raiz nona primitiva da unidade

$$\eta = \cos \frac{2\pi}{9} + i \sin \frac{2\pi}{9},$$

logo é raiz trigésima sexta primitiva da unidade o número complexo

$$\xi\eta = -\sin \frac{2\pi}{9} + i \cos \frac{2\pi}{9}.$$

Problemas

5.1 Sejam ξ_λ com $\lambda = 0, 1, \dots, n-1$ as raízes n -ésimas da unidade em \mathbb{C} e seja m um inteiro qualquer. Calcule:

- (a) $\xi_0^m + \xi_1^m + \cdots + \xi_{n-1}^m$;
- (b) $\xi_0^m \cdot \xi_1^m \cdots \xi_{n-1}^m$.

5.2 Seja $\xi \neq 1$ uma raiz n -ésima da unidade. Mostre que ξ é raiz da equação

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

5.3 Seja $p > 1$ um número primo. Mostre que

- (a) Toda raiz p -ésima da unidade diferente de 1 é primitiva;
- (b) As raízes p^α -ésimas da unidade não primitivas são raízes $p^{\alpha-1}$ -ésimas da unidade.

5.4 Seja ξ uma raiz n -ésima primitiva da unidade. Mostre que ξ^m é uma raiz n -ésima primitiva da unidade para algum inteiro m se e somente se $(m, n) = 1$.

5.5 Prove que as raízes n -ésimas primitivas da unidade são duas a duas conjugadas.

5.6 Seja ξ uma raiz n -ésima da unidade. Considere o conjunto

$$P(\xi) = \{m \in \mathbb{Z} \mid \xi^m = 1\}.$$

- a) Mostre que $P(\xi)$ é um ideal não nulo de \mathbb{Z} . Se p é o gerador positivo de $P(\xi)$, então p é chamado de período de ξ .
- b) Se ξ é uma raiz primitiva, qual é o seu período.
- c) Mostre que $\xi^m = 1$ se e somente se $p \mid m$. Em particular conclua que $p \mid n$.
- d) Mostre que o período de uma raiz ξ_λ é precisamente $\frac{n}{(\lambda, n)}$.

5.7 Com as definições do Problema 5.6, calcule o período da raiz

- a) décimo segunda da unidade ξ_8 ;
- b) trigésima da unidade ξ_{12} ;
- c) n -ésima da unidade ξ_1 .

5.8 Sejam $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ e $\rho = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ respectivamente raízes primitivas cúbica e oitava da unidade. Ache valores para λ e μ inteiros de modo que

$$\cos 15^\circ + i \sin 15^\circ = \omega^\lambda \rho^\mu.$$

Use este resultado para calcular $\cos 15^\circ$ e $\sin 15^\circ$.

5.9 Seja $z = \cos \theta + i \sin \theta$, com $\theta \in \mathbb{R}$. Mostre que as seguintes condições são equivalentes

- i) z é raiz da unidade;
- ii) $\frac{\theta}{2\pi} \in \mathbb{Q}$;
- iii) o conjunto $\{z^n \mid n \in \mathbb{Z}\}$ é finito.

Os Inteiros Gaussianos

Para resolver o problema da reciprocidade biquadrática, Gauss introduziu num trabalho publicado em 1825 os números complexos da forma $a + bi$ com a e b inteiros. Estes números, chamados de inteiros gaussianos, possuem propriedades muito semelhantes às dos números inteiros conforme veremos no decorrer do presente capítulo.

1. O Anel dos Inteiros Gaussianos

Um *inteiro gaussiano* é um número complexo da forma $a + bi$ com a e b inteiros.

Proposição 1. *O conjunto dos inteiros gaussianos é um subanel de \mathbb{C} .*

Demonstração: É claro que $1 = 1 + 0i$ é um inteiro gaussiano. Sejam $z = a + bi$ e $z' = a' + b'i$ dois inteiros gaussianos, isto é, $a, b, a', b' \in \mathbb{Z}$, então $z - z'$ e $z \cdot z'$ são inteiros gaussianos pois

$$\begin{aligned} z - z' &= (a - a') + (b - b')i, \\ z \cdot z' &= (aa' - bb') + (ab' + a'b)i, \end{aligned}$$

onde $(a - a')$, $(b - b')$, $(aa' - bb')$ e $(ab' + a'b)$ são inteiros. Logo o resultado segue pela Proposição 1 do Capítulo 7. \square

O anel dos inteiros gaussianos será denotado por $\mathbb{Z}[i]$. Note que esta notação já foi usada no Capítulo 7 para representar o subanel de \mathbb{C} gerado por \mathbb{Z} e por i . Isto não é inconveniente pois de fato o anel dos inteiros gaussianos por conter i e \mathbb{Z} e estar contido no anel gerado por \mathbb{Z} e i , coincide com este último.

Considere a seguinte função

$$\begin{aligned} N: \mathbb{C} &\longrightarrow \mathbb{R}^+ \\ a + bi &\longmapsto |a + bi|^2 = a^2 + b^2 \end{aligned}$$

Esta função é chamada de *função norma* e em decorrência da Proposição 1 do Capítulo 9, possui a propriedade seguinte,

$$N(z \cdot z') = N(z) \cdot N(z'),$$

quaisquer que sejam $z, z' \in \mathbb{C}$. Note que se $\alpha \in \mathbb{Z}[i]$, então $N(\alpha) \in \mathbb{Z}^+$.

O próximo resultado nos caracterizará os elementos invertíveis de $\mathbb{Z}[i]$.

Proposição 2. *Seja $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:*

- (i) α é invertível em $\mathbb{Z}[i]$;
- (ii) $N(\alpha) = 1$;
- (iii) $\alpha \in \{-1, 1, -i, i\}$.

Demonstração: (i) \Rightarrow (ii): Sendo α invertível, existe $\beta \in \mathbb{Z}[i]$ tal que

$$\alpha \cdot \beta = 1.$$

Consequentemente,

$$N(\alpha) \cdot N(\beta) = N(\alpha \cdot \beta) = N(1) = 1.$$

Como $N(\alpha) \in \mathbb{Z}^+$, segue das igualdades acima que $N(\alpha) = 1$.

(ii) \Rightarrow (iii): Suponhamos $N(\alpha) = 1$. Pondo $\alpha = x + yi$, temos que

$$x^2 + y^2 = 1,$$

cujas soluções em $\mathbb{Z} \times \mathbb{Z}$ são $(0, \pm 1)$ e $(\pm 1, 0)$. Portanto $\alpha \in \{-1, 1, -i, i\}$.

(iii) \Rightarrow (i): É claro que todo elemento de $\{-1, 1, -i, i\}$ é invertível em $\mathbb{Z}[i]$. \square

O anel dos inteiros gaussianos possui propriedades algébricas e aritméticas muito semelhantes às do anel dos inteiros e a razão disto

se deve em parte ao fato que em $\mathbb{Z}[i]$ tem-se uma divisão com resto “pequeno” semelhante à divisão euclidiana em \mathbb{Z} .

Proposição 3 (divisão com resto). *Sejam $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$. Então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que:*

$$\alpha = \beta \cdot \gamma + \rho, \text{ com } N(\rho) < N(\beta).$$

Demonstração: Trata-se de achar um inteiro gaussiano γ tal que

$$N(\alpha - \beta\gamma) < N(\beta)$$

como

$$N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\alpha - \beta\gamma),$$

segue que devemos achar um inteiro gaussiano γ tal que

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < 1.$$

Escrevendo $\frac{\alpha}{\beta}$ na forma normal, é fácil ver que existem $x, y \in \mathbb{Q}$ tais que

$$\frac{\alpha}{\beta} = x + yi.$$

Sejam r e s inteiros tais que

$$|x - r| \leq \frac{1}{2} \quad \text{e} \quad |y - s| \leq \frac{1}{2},$$

(tais inteiros existem em decorrência da Observação 5 após o Teorema 6 do Capítulo 3). Pondo $\gamma = r + si$ e $\rho = \alpha - \beta\gamma$, segue que

$$\alpha = \beta \cdot \gamma + \rho,$$

com

$$\begin{aligned} N(\rho) &= N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\beta) \cdot N(x - r + (y - s)i) \\ &= N(\beta)[(x - r)^2 + (y - s)^2] \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) \\ &= \frac{1}{2}N(\beta) < N(\beta). \end{aligned} \quad \square$$

Note que na proposição acima nada afirmamos à respeito da unicidade de γ e ρ .

Exemplo: Dividiremos $\alpha = 4 + 5i$ por $\beta = 1 + i$ em $\mathbb{Z}[i]$. Temos que

$$\frac{\alpha}{\beta} = \frac{4 + 5i}{1 + i} = \frac{(1 - i)(4 + 5i)}{2} = \frac{9 + i}{2} = \frac{9}{2} + \frac{1}{2}i.$$

Pela construção acima, $\gamma = r + si$ onde r e s satisfazem as desigualdades

$$\left| \frac{9}{2} - r \right| \leq \frac{1}{2} \quad \text{e} \quad \left| \frac{1}{2} - s \right| \leq \frac{1}{2}$$

Temos as seguintes possibilidades: $r \in \{4, 5\}$ e $s \in \{0, 1\}$. Portanto, os possíveis pares solução (γ, ρ) com $\gamma = r + si$ e $\rho = \alpha - \beta \cdot \gamma$ são

$$(4, i), (4 + i, 1), (5, -1) \text{ e } (5 + i, -i).$$

O fato de termos em $\mathbb{Z}[i]$ uma divisão com resto, implica como no caso de \mathbb{Z} que $\mathbb{Z}[i]$ é principal como demonstramos a seguir.

Teorema 1. $\mathbb{Z}[i]$ é um domínio principal.

Demonstração: Seja I um ideal de $\mathbb{Z}[i]$. Se $I = (0)$, nada temos a provar. Suponha que $I \neq (0)$. Considere o conjunto

$$\Lambda = \{N(z) \mid z \in I \setminus \{0\}\}.$$

Este é um subconjunto não vazio de \mathbb{N} , logo possui um menor elemento $n \in \mathbb{N}$. Seja $\alpha \in I \setminus \{0\}$ tal que $N(\alpha) = n$. Vamos provar que $I = I(\alpha)$.

De fato, dado que $\alpha \in I$, segue que $I(\alpha) \subset I$. Por outro lado, se $z \in I$, então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que

$$z = \alpha \cdot \gamma + \rho \text{ com } N(\rho) < N(\alpha).$$

Suponha por absurdo que $\rho \neq 0$, logo

$$\rho = z - \alpha \cdot \gamma \in I$$

com $0 < N(\rho) < N(\alpha) = n$, o que é uma contradição pela escolha de α . Isto implica que $z = \alpha \cdot \gamma \in I(\alpha)$, consequentemente $I \subset I(\alpha)$ e portanto $I = I(\alpha)$. \square

Destacamos os seguintes corolários do teorema acima chamando a atenção de que tudo que foi enunciado e provado para domínios principais vale em $\mathbb{Z}[i]$.

Corolário 1. *Dados $\alpha_1, \dots, \alpha_s \in \mathbb{Z}[i]$, existe um máximo divisor comum destes elementos e todo mdc é da forma $n_1\alpha_1 + \dots + n_s\alpha_s$ com $n_1, \dots, n_s \in \mathbb{Z}[i]$.*

Demonstração: Isto foi provado no Corolário 1 da Proposição 6, Capítulo 4. \square

Corolário 2. $\mathbb{Z}[i]$ é domínio de fatoração única.

Demonstração: Isto é consequência do teorema acima e do Teorema 2 do Capítulo 4. \square

A virtude da demonstração da Proposição 3 é que nos mostra que a divisão com resto em $\mathbb{Z}[i]$ é algorítmica. Isto permite calcular efetivamente o mdc de dois elementos pelo método de Euclides que apresentamos para os inteiros no Capítulo 5. Poderemos em consequência resolver efetivamente equações diofantinas lineares.

Note que dado $\delta \in \mathbb{Z}[i]$ tal que $\delta \neq 0$, então um e somente um dos quatro associados δ' de δ é tal que,

$$\operatorname{Re}\delta' > 0 \quad \text{e} \quad \operatorname{Im}\delta' \geq 0.$$

Dados $\alpha, \beta \in \mathbb{Z}[i]$ não ambos nulos, vamos denotar por (α, β) o mdc δ de α e β tal que $\operatorname{Re}\delta > 0$ e $\operatorname{Im}\delta \geq 0$.

Exemplo: Considere a equação diofantina

$$(14i - 8)x + (5 + 5i)y = 23i - 1.$$

Pelo algoritmo de Euclides temos

$$\begin{aligned} 14i - 8 &= (5 + 5i)(1 + 2i) + (-3 - i) \\ 5 + 5i &= (-3 - i)(-2 - i) + 0, \end{aligned}$$

logo $-3 - i$ é um mdc de $14i - 8$ e $5 + 5i$ e consequentemente,

$$(14i - 8, 5 + 5i) = 3 + i.$$

Como $23i - 1 = (3 + i)(7i + 2)$, segue que $(3 + i) \mid (23i - 1)$ e portanto a equação admite solução (Veja Teorema 3, Capítulo 5).

Usando o algoritmo de Euclides de trás para frente, temos que

$$3 + i = -(14i - 8) + (5 + 5i)(1 + 2i),$$

logo

$$(23i - 1) = (7i + 2)(3 + i) = -(7i + 2)(14i - 8) + (7i + 2)(1 + 2i)(5 + 5i).$$

Daí segue que uma solução particular da equação diofantina é

$$x_0 = -(7i + 2),$$

$$y_0 = (7i + 2)(1 + 2i) = 11i - 12$$

Portanto, pelo Teorema 4 do Capítulo 5 adaptado para $\mathbb{Z}[i]$, temos que a solução geral da equação diofantina é

$$x = -(7i + 2) + (t + si) \frac{5 + 5i}{3 + i} = -(7i + 2) + (t + si)(2 + i)$$

$$y = (11i - 12) - (t + si) \frac{14i - 8}{3 + i} = 11i - 12 - (t + si)(5i - 1)$$

com $t, s \in \mathbb{Z}$.

Problemas

1.1 Seja $\mathbb{Q}(i)$ o subcorpo de \mathbb{C} gerado por \mathbb{Q} e por i

- a) Mostre que $\mathbb{Q}(i) = \{x + yi \mid x, y \in \mathbb{Q}\}$;
- b) Mostre que $\mathbb{Q}(i)$ é o corpo de frações de $\mathbb{Z}[i]$.

1.2 Resolva as seguintes equações diofantinas

- a) $(16 + 7i)x + (10 - 5i)y = 15 + 5i$;
- b) $(4 + 6i)x + (5 - 15i)y = i$.

1.3 Sejam $\alpha, \beta \in \mathbb{Z}[i]$. Mostre que se $\alpha \mid \beta$, então $N(\alpha) \mid N(\beta)$.

1.4 Mostre que dado um inteiro gaussiano $\delta \neq 0$, existe um único elemento δ' de $\mathbb{Z}[i]$ associado de δ tal que $\operatorname{Re} \delta' > 0$ e $\operatorname{Im} \delta' \geq 0$.

1.5 Mostre que 2 é associado de um quadrado em $\mathbb{Z}[i]$.

1.6 Seja A um anel e $f: \mathbb{Z}[i] \rightarrow A$ um homomorfismo de anéis.

a) Mostre que existe $\varepsilon \in A$ com $\varepsilon^2 = -1$ tal que

$$f(a + bi) = a1 + b\varepsilon.$$

b) Mostre que só existem dois homomorfismos de anéis de $\mathbb{Z}[i]$ em \mathbb{C} , a identidade e a conjugação.

c) Mostre que não existem homomorfismos de anéis de $\mathbb{Z}[i]$ em \mathbb{R} .

2. Elementos Primos de $\mathbb{Z}[i]$

Nesta seção determinaremos os elementos primos de $\mathbb{Z}[i]$. Observe que sendo $\mathbb{Z}[i]$ um domínio principal, os conceitos de elemento primo e elemento irredutível coincidem (Veja Proposições 8 e 9 do Capítulo 4).

Lema 1. *Todo elemento primo de $\mathbb{Z}[i]$ divide um número primo de \mathbb{Z} .*

Demonstração: Seja π um elemento primo de $\mathbb{Z}[i]$ e considere a decomposição em \mathbb{Z} de $N(\pi)$ em fatores primos,

$$N(\pi) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Como $N(\pi) = \pi \cdot \bar{\pi}$, segue que $\pi | N(\pi)$ e como π é primo, ele divide um dos fatores $p_j^{\alpha_j}$ e portanto divide o primo p_j . \square

Lema 2. *Seja $\pi \in \mathbb{Z}[i]$. Se $N(\pi)$ é primo em \mathbb{Z} , então π é primo em $\mathbb{Z}[i]$.*

Demonstração: Suponha que $\pi \neq 0$ não seja primo em $\mathbb{Z}[i]$. Temos então que $\pi = \pi_1 \cdot \pi_2$ com π_1 e π_2 não nulos e não invertíveis, logo

$$N(\pi) = N(\pi_1) \cdot N(\pi_2)$$

com $N(\pi_1) > 1$ e $N(\pi_2) > 1$ (veja Proposição 2). Portanto $N(\pi)$ não é primo em \mathbb{Z} . Isto prova a asserção. \square

Exemplos

1. O número inteiro 2 não é primo em $\mathbb{Z}[i]$. De fato, sendo $N(1+i) =$

$N(1 - i) = 2$, temos pelo Lema 2 que $1 + i$ e $1 - i$ são primos em $\mathbb{Z}[i]$. Portanto uma decomposição de 2 em fatores primos em $\mathbb{Z}[i]$ é dada por

$$2 = (1 + i)(1 - i)$$

2. O número inteiro 5 não é primo em $\mathbb{Z}[i]$ e uma sua decomposição em fatores primos é dada por

$$5 = (1 + 2i)(1 - 2i).$$

Um número inteiro n será dito *soma de dois quadrados* se existirem inteiros a e b tais que $n = a^2 + b^2$. Em particular, todo quadrado a^2 é soma de dois quadrados pois $a^2 = a^2 + 0^2$.

Lema 3. *Seja p um número primo de \mathbb{Z} . As seguintes asserções são equivalentes*

- (i) p é redutível em $\mathbb{Z}[i]$;
- (ii) $p = \alpha \cdot \bar{\alpha}$ com α primo em $\mathbb{Z}[i]$;
- (iii) p é soma de dois quadrados.

Demonstração: (i) \Rightarrow (ii): Suponha que p é redutível em $\mathbb{Z}[i]$, logo $p = \alpha \cdot \beta$ com $\alpha, \beta \in \mathbb{Z}[i]$ não invertíveis. Como

$$p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta),$$

temos que $N(\alpha) = N(\beta) = p$, logo pelo Lema 2, temos que α é primo em $\mathbb{Z}[i]$. Por outro lado,

$$\beta = \frac{p}{\alpha} = \frac{p \cdot \bar{\alpha}}{N(\alpha)} = \bar{\alpha},$$

logo $p = \alpha \cdot \beta = \alpha \cdot \bar{\alpha}$.

(ii) \Rightarrow (iii): Suponha que $p = \alpha \cdot \bar{\alpha}$. Se $\alpha = a + bi$, segue que

$$p = \alpha \cdot \bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2,$$

e portanto p é soma de dois quadrados.

(iii) \Rightarrow (i): Se $p = a^2 + b^2$, logo $p = (a + bi)(a - bi)$. Como

$$p^2 = N(p) = N(a + bi)N(a - bi),$$

e como $N(a + bi) = N(a - bi)$, temos que

$$N(a + bi) = N(a - bi) = p.$$

Consequentemente pela Proposição 2, temos que $a + bi$ e $a - bi$ não são invertíveis, provando assim que p é redutível em $\mathbb{Z}[i]$. \square

O nosso objetivo agora é caracterizar os números primos que são somas de dois quadrados.

Um número inteiro a será dito *resíduo quadrático* módulo um inteiro m , se \bar{a} for um quadrado em \mathbb{Z}_m .

Lema 4. *Qualquer que seja o número primo p com $p > 2$, existe um inteiro em \mathbb{Z} que não é resíduo quadrático módulo p .*

Demonstração: Suponha que $\bar{1}, \bar{2}, \dots, \bar{p-1}$ sejam todos quadrados em \mathbb{Z}_p , logo

$$\{\bar{1}, \bar{2}, \dots, \bar{p-1}\} = \{\bar{1}^2, \bar{2}^2, \dots, \bar{p-1}^2\},$$

e consequentemente,

$$1 \cdot 2 \cdots (p-1) \equiv 1^2 \cdot 2^2 \cdots (p-1)^2 \pmod{p}.$$

Pelo Teorema de Wilson (Teorema 1, Capítulo 6), temos que

$$-1 \equiv (-1)^2 \pmod{p},$$

e portanto $p = 2$; contradição. \square

Lema 5. *Sejam p um número primo com $p > 2$ e a um inteiro não resíduo quadrático módulo p . Então*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Demonstração: Como \mathbb{Z}_p é um corpo, para cada $a' \in \{1, 2, \dots, p-1\}$, existe um único $a'' \in \{1, 2, \dots, p-1\}$ tal que

$$\bar{a'} \cdot \bar{a''} = \bar{a} \tag{1}$$

Como \bar{a} não é resíduo quadrático módulo p , temos que $a' \neq a''$. Considere agora todos os possíveis tais pares não ordenados $\{a', a''\}$.

Temos $\frac{p-1}{2}$ tais pares. Multiplicando membro a membro todas as igualdades (1) ao variar de $\{a', a''\}$, temos que

$$\overline{(p-1)!} = (\bar{a})^{\frac{p-1}{2}},$$

logo pelo Teorema de Wilson (Teorema 1, Capítulo 6), temos que

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad \square$$

Teorema 2 (Fermat). *Seja p um número primo em \mathbb{Z} . As seguintes asserções são equivalentes*

- (i) p é soma de dois quadrados;
- (ii) $p = 2$ ou $p \equiv 1 \pmod{4}$;
- (iii) -1 é resíduo quadrático módulo p .

Demonstração: (i) \Rightarrow (ii): Suponha que $p = a^2 + b^2$. Supondo $p > 2$, vamos provar que $p \equiv 1 \pmod{4}$. Como p é um primo não par, temos que a e b são de paridade diferente, portanto

$$p = a^2 + b^2 = (2n+1)^2 + (2m)^2,$$

e consequentemente, $p \equiv 1 \pmod{4}$.

(ii) \Rightarrow (iii): Se $p = 2$, então $-1 \equiv 1 \pmod{2}$ e portanto -1 é resíduo quadrático módulo 2. Suponha agora que $p \equiv 1 \pmod{4}$. Seja a um inteiro que não é resíduo quadrático módulo p (tal inteiro existe em virtude do Lema 4). Como $p \equiv 1 \pmod{4}$, temos que $b = a^{\frac{p-1}{4}}$ é um inteiro e pelo Lema 5,

$$b^2 = a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

e consequentemente -1 é um resíduo quadrático módulo p .

(iii) \Rightarrow (i): Suponha que existe $b \in \mathbb{Z}$ tal que

$$b^2 \equiv -1 \pmod{p}.$$

Logo p divide $b^2 + 1$ e portanto

$$p \mid (b+i)(b-i).$$

Note que $p \nmid (b \pm i)$ pois caso contrário teríamos para algum $t + si \in \mathbb{Z}[i]$ que $p(t + si) = b \pm i$, o que implica que $ps = \pm 1$, absurdo.

Temos então que p não é primo em $\mathbb{Z}[i]$ e portanto redutível. Pelo Lema 3 temos que p é soma de dois quadrados. \square

Corolário. *Os elementos primos de $\mathbb{Z}[i]$ são*

- a) *Os associados dos primos p de \mathbb{Z} tais que $p \equiv 3 \pmod{4}$;*
- b) *Os elementos da forma $a + bi$ tais que $a^2 + b^2$ é primo em \mathbb{Z} .*

Demonstração: Pelo Lema 1 temos que todo primo π de $\mathbb{Z}[i]$ é divisor primo de um número primo p de \mathbb{Z} . Se p não é soma de dois quadrados, pelo Lema 3, temos que p é irreduzível em $\mathbb{Z}[i]$, logo primo e isto ocorre se e somente se $p \equiv 3 \pmod{4}$. Neste caso π é associado de p .

Se $p = 2$ ou $p \equiv 1 \pmod{4}$, então pelo Teorema 2 temos que p é soma de dois quadrados e portanto pelo Lema 3, temos que $\pi = a + bi$ tal que $a^2 + b^2 = p$. \square

O Teorema 2 pode ser enunciado do seguinte modo. Seja p um número primo de \mathbb{Z} . A equação

$$x^2 + y^2 = p$$

tem solução em \mathbb{Z} se e somente se $p = 2$ ou $p \equiv 1 \pmod{4}$.

A fim de generalizar o resultado acima necessitaremos do seguinte lema

Lema 6. (a) *Tem-se que $n \in \mathbb{Z}$ é soma de dois quadrados se e somente se existe $\alpha \in \mathbb{Z}[i]$ tal que $n = N(\alpha)$.*

(b) *Dados inteiros que são somas de dois quadrados, o seu produto é soma de dois quadrados.*

Demonstração: (a) Tem-se que $n = a^2 + b^2$ se e somente se $n = N(\alpha)$ onde $\alpha = a + bi$.

(b) Suponha que n_1, \dots, n_r são somas de dois quadrados, logo $n_1 = N(\alpha_1), \dots, n_r = N(\alpha_r)$ com $\alpha_1, \dots, \alpha_r \in \mathbb{Z}[i]$. Temos então que

$$n_1 \cdots n_r = N(\alpha_1) \cdots N(\alpha_r) = N(\alpha_1 \cdots \alpha_r),$$

e consequentemente $n_1 \cdots n_r$ é soma de dois quadrados. \square

Teorema 3 (Fermat). Seja $n \in \mathbb{N}$ com decomposição em fatores primos dada por

$$n = 2^\alpha \cdot p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s},$$

onde cada p_i é um primo com $p_i \equiv 1 \pmod{4}$ e cada q_j é um primo com $q_j \equiv 3 \pmod{4}$. A equação $x^2 + y^2 = n$ tem solução em \mathbb{Z} (isto é, n é soma de dois quadrados) se e somente se $\gamma_1, \dots, \gamma_s$ são pares.

Demonstração: Como 2 e todo primo p com $p \equiv 1 \pmod{4}$ são pelo Teorema 2 somas de dois quadrados e todo inteiro elevado a um expoente par é um quadrado, logo soma de dois quadrados, temos pelo Lema 6 que os números da forma

$$n = 2^\alpha p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s}$$

com os γ_j pares, são somas de dois quadrados.

Reciprocamente, seja n como no enunciado e suponha que um dos γ_j seja ímpar, que sem perda de generalidade podemos supor ser γ_1 . Suponhamos que $n = a^2 + b^2$ e seja $d = (a, b)$. Temos que $a = da_1$ e $b = db_1$ com $(a_1, b_1) = 1$. Logo

$$n = d^2(a_1^2 + b_1^2).$$

Como a maior potência de q_1 que divide d^2 tem expoente par e γ_1 é ímpar, temos que $q_1 \mid (a_1^2 + b_1^2)$. Consequentemente,

$$a_1^2 + b_1^2 \equiv 0 \pmod{q_1}. \quad (1)$$

Como $(a_1, b_1) = 1$, temos que $(a_1, q_1) = 1$ ou $(b_1, q_1) = 1$. Digamos que $(a_1, q_1) = 1$ (o outro caso é análogo). Logo $\bar{a}_1 \neq \bar{0}$ em \mathbb{Z}_{q_1} e de (1) segue que

$$\bar{b}_1^2(\bar{a}_1^2)^{-1} + \bar{1} = \bar{0}. \quad (2)$$

Seja $c \in \mathbb{Z}$ tal que $\bar{c} = \bar{b}_1(\bar{a}_1)^{-1}$, logo de (2) temos que

$$\bar{c}^2 = -\bar{1},$$

e consequentemente pelo Teorema 2 temos que $q_1 = 2$ ou $q_1 \equiv 1 \pmod{4}$, contradição. \square

Problemas

2.1 Decomponha os seguintes números em fatores primos em $\mathbb{Z}[i]$

- a) 7×5 b) 11×13 c) $5 + 7i$ d) $7 + 5i$

2.2 Decomponha $66 + 162i$ em fatores primos em $\mathbb{Z}[i]$.

2.3 Ache os resíduos quadráticos módulo 5; idem módulo 7.

2.4 Quais são os inteiros abaixo que são somas de dois quadrados

- a) $2^3 \times 5^2 \times 7$ b) $2 \times 3^2 \times 5 \times 7^4$ c) $3^2 \times 5 \times 13^3$

2.5 Escreva 425 como soma de dois quadrados.

2.6 Mostre que 2 é o único número primo de \mathbb{Z} que é associado de um quadrado de $\mathbb{Z}[i]$

3. A Equação Pitagórica

Nesta seção resolveremos em \mathbb{Z} a chamada equação pitagórica,

$$x^2 + y^2 = z^2.$$

Para tanto necessitaremos do seguinte lema

Lema 7. Sejam x e y inteiros primos entre si, então

$$(x + yi, x - yi) = \begin{cases} 1 & , \text{se } x^2 + y^2 \text{ é ímpar} \\ 1 + i & , \text{se } x^2 + y^2 \text{ é par} \end{cases}$$

Demonstração: Observe inicialmente que sendo x e y primos entre si em \mathbb{Z} , existem inteiros m e n tais que $mx + ny = 1$, logo x e y são primos entre si em $\mathbb{Z}[i]$. Note também que como $N(x + yi) = N(x - yi)$, então $x + yi$ e $x - yi$ são simultaneamente invertíveis ou não invertíveis.

Seja $\alpha \in \mathbb{Z}[i]$ tal que α divide simultaneamente $x + yi$ e $x - yi$. Logo α divide a soma $2x$ e a diferença $2y$ destes números. Como x e y são primos entre si em $\mathbb{Z}[i]$, temos que $\alpha | 2$ e consequentemente α é associado de 1, $1 + i$ ou 2.

Não podemos ter 2 dividindo simultaneamente $x + yi$ e $x - yi$ pois teríamos $4 | (x + yi)(x - yi)$ e consequentemente $x^2 + y^2 \equiv 0 \pmod{4}$. Isto é impossível pois sendo x e y primos entre si, eles são de paridade distinta ou ambos ímpares e isto implica que $x^2 + y^2 \equiv 1, 2 \pmod{4}$.

Suponha que $x^2 + y^2$ seja par, logo $2 \mid (x + yi)(x - yi)$, portanto $x + yi$ e $x - yi$ não são invertíveis e $i(1+i)^2 \mid (x+yi)(x-yi)$, logo $(1+i) \mid (x+yi)$ e $(1+i) \mid (x-yi)$ e neste caso,

$$(x+yi, x-yi) = 1+i.$$

Suponha agora que $x^2 + y^2$ seja ímpar. Se $(1+i) \mid (x+yi)$, segue que $(1-i) \mid (x-yi)$, logo $2 \mid x^2 + y^2$; absurdo. Portanto, $(x+yi, x-yi) = 1$. \square

Teorema 4. As soluções (x, y, z) da equação $x^2 + y^2 = z^2$ com x e y primos entre si são todas as ternas da forma $(\pm(a^2 - b^2), \pm 2ab, \pm(a^2 + b^2))$ ou $(\pm 2ab, \pm(a^2 - b^2), \pm(a^2 + b^2))$ com $a, b \in \mathbb{Z}$, primos entre si e de paridade distinta.

Demonstração: Seja (x, y, z) uma solução de $x^2 + y^2 = z^2$ com x e y primos entre si. Como todo quadrado em \mathbb{Z} é congruente a 0 ou 1 módulo 4 (verifique), temos que $x^2 + y^2 \equiv 0, 1 \pmod{4}$. Não podemos ter $x^2 + y^2 \equiv 0 \pmod{4}$ pois teríamos x e y pares (verifique), o que não ocorre pois x e y são primos entre si. Portanto $x^2 + y^2 \equiv 1 \pmod{4}$. Em particular, $x^2 + y^2$ é ímpar e pelo Lema 7, temos que $x + yi$ e $x - yi$ são relativamente primos. Seja $z = \pi_1^{n_1} \cdots \pi_r^{n_r}$ a decomposição de z em fatores primos, logo

$$(x+yi)(x-yi) = \pi_1^{2n_1} \cdots \pi_r^{2n_r}$$

Como $x + yi$ e $x - yi$ são primos entre si, devemos ter que $x + yi$ é associado de um quadrado,

$$x + yi = u(a + bi)^2,$$

com u invertível em $\mathbb{Z}[i]$. Segue daí, segundo os valores de u , que

$$x = \pm(a^2 - b^2) \text{ e } y = \pm 2ab$$

ou

$$x = \pm 2ab \text{ e } y = \pm(a^2 - b^2).$$

Calculando z a partir da equação $x^2 + y^2 = z^2$, obtemos $z = \pm(a^2 + b^2)$.

Reciprocamente, é imediato verificar que todas as ternas como no enunciado são soluções da equação proposta. \square

Problemas

3.1 Determine todas as ternas de inteiros que representam as medidas dos lados de um triângulo retângulo cujo perímetro é inferior a 20 unidades de medida.

3.2 Resolva em inteiros a equação $x^2 + y^2 = 2z^2$.

4. Quocientes do Anel de Inteiros Gaussianos

Sendo $\mathbb{Z}[i]$ principal, os seus ideais são da forma $I(\alpha)$ com $\alpha = a+bi \in \mathbb{Z}[i]$. Nesta seção estudaremos os anéis quocientes da forma $\mathbb{Z}[i]/I(\alpha)$. Inicialmente, vamos determinar o número de elementos de tal anel. Dado $\beta \in \mathbb{Z}[i]$ usaremos nesta seção a notação $\bar{\beta}$ para representar a classe de β em $\mathbb{Z}[i]/I(\alpha)$ e não o conjugado de β .

Proposição 4. Sejam $\alpha = a+bi \in \mathbb{Z}[i] \setminus \{0\}$ e $d = mdc(a, b)$. Então tem-se uma bijeção entre $\mathbb{Z}[i]/I(\alpha)$ e o conjunto

$$\Lambda = \left\{ r + si \in \mathbb{Z}[i] \mid r = 0, 1, \dots, \frac{N(\alpha)}{d} - 1, s = 0, 1, \dots, d - 1 \right\}$$

Demonstração: A asserção segue do fato que em cada classe residual $e + fi$ de $\mathbb{Z}[i]/I(\alpha)$ existe um único inteiro gaussiano pertencente ao conjunto Λ . É precisamente isto que iremos verificar.

Um elemento qualquer $x + yi$ da classe $\bar{e+fi}$ é da forma,

$$x + yi = (a + bi)(u + vi) + e + fi. \quad (1)$$

Da equação (1) acima obtemos as seguintes equações

$$x = au - bv + e \quad (2)$$

$$y = av + bu + f \quad (3)$$

Como o inteiro $av + bu$ é divisível por d , quaisquer que sejam $u, v \in \mathbb{Z}$, temos que

$$y \equiv f \pmod{d}.$$

Portanto, existe um único inteiro $s \in \{0, 1, \dots, d - 1\}$ tal que pondo $y = s$, a equação (3) admita soluções em u e v . Seja u_0, v_0 uma solução particular da equação (3) com $y = s$. Segue do Teorema 4, Capítulo 5, que a solução geral desta equação é dada, para $t \in \mathbb{Z}$, por

$$\begin{cases} u = u_0 + \frac{a}{d}t \\ v = v_0 - \frac{b}{d}t \end{cases}$$

Substituindo estas expressões de u e v em (2) temos que

$$x = au_0 - bv_0 + e + \frac{a^2 + b^2}{d}t \quad (4)$$

Como $\frac{a^2 + b^2}{d} = \frac{N(\alpha)}{d} \in \mathbb{Z}$, segue que

$$x \equiv au_0 - bv_0 + e \pmod{\frac{N(\alpha)}{d}},$$

e consequentemente existe um único inteiro $r \in \left\{0, 1, \dots, \frac{N(\alpha)}{d} - 1\right\}$ tal que pondo $x = r$, a equação (4) admita solução em t . Isto conclui a demonstração da proposição. \square

Corolário. Seja $\alpha \in \mathbb{Z}[i] \setminus \{0\}$. Então o anel quociente $\mathbb{Z}[i]/I(\alpha)$ possui $N(\alpha)$ elementos.

Demonstração: Pela Proposição 4, temos que o número de elementos de $\mathbb{Z}[i]/I(\alpha)$ é igual ao número de elementos de Λ que é precisamente $\frac{N(\alpha)}{d} \cdot d = N(\alpha)$. \square

Exemplos

1. Seja $\alpha = 1 + i$. Temos que $N(\alpha) = 2$ e $d = 1$, logo $\mathbb{Z}[i]/I(\alpha)$ tem apenas duas classes residuais que são $\bar{0}$ e $\bar{1}$.
2. Seja $\alpha = 5$. Temos que $N(\alpha) = 25$ e $d = 5$, logo $\mathbb{Z}[i]/I(\alpha)$ tem 25 classes residuais dadas por $\bar{r+si}$ com $r, s \in \{0, 1, 2, 3, 4\}$.
3. Seja $\alpha = 5 + 10i$. Temos que $N(\alpha) = 125$ e $d = 5$, logo $\mathbb{Z}[i]/I(\alpha)$ tem 125 classes residuais dadas por $\bar{r+si}$ com $r = \{0, 1, \dots, 24\}$ e $s \in \{0, 1, 2, 3, 4\}$.

4. Se $\alpha = a + bi$ com $(a, b) = 1$, então $\mathbb{Z}[i]/I(\alpha)$ tem $a^2 + b^2$ elementos dados por

$$\overline{0}, \overline{1}, \overline{2}, \dots, \overline{a^2 + b^2 - 1}.$$

Iremos agora estudar os elementos invertíveis dos anéis do tipo $\mathbb{Z}[i]/I(\alpha)$.

Inicialmente caracterizaremos os quocientes de $\mathbb{Z}[i]$ que são corpos. Pela Proposição 14 do Capítulo 7, temos que $\mathbb{Z}[i]/I(\alpha)$ é um corpo se e somente se $I(\alpha)$ é um ideal maximal de $\mathbb{Z}[i]$ e isto por sua vez é equivalente, em virtude da Proposição 11 do Capítulo 7, a que α seja um elemento primo de $\mathbb{Z}[i]$. A discussão acima, juntamente com o Corolário do Teorema 2, prova a seguinte proposição.

Proposição 5. $\mathbb{Z}[i]/I(\alpha)$ é um corpo se e somente se α é associado de um primo p de \mathbb{Z} tal que $p \equiv 1 \pmod{4}$, ou $\alpha = a + bi$ tal que $a^2 + b^2$ é primo em \mathbb{Z} .

Temos a seguinte caracterização dos elementos invertíveis de um quociente $\mathbb{Z}[i]/I(\alpha)$.

Proposição 6. Sejam $\alpha, \beta \in \mathbb{Z}[i]$. Temos que $\overline{\beta}$ é invertível em $\mathbb{Z}[i]/I(\alpha)$ se e somente se $(\alpha, \beta) = 1$ em $\mathbb{Z}[i]$.

Demonstração: Análogo à demonstração da Proposição 6 do Capítulo 6. \square

Introduzimos agora uma função chamada de *função Φ de Gauss*, análoga à função Φ de Euler que designaremos com a mesma letra Φ

$$\begin{aligned} \Phi: \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\} &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto \text{número de elementos invertíveis} \\ &\quad \text{de } \mathbb{Z}[i]/I(\alpha) \end{aligned}$$

É claro que se π é um elemento primo de $\mathbb{Z}[i]$, então $\mathbb{Z}[i]/I(\pi)$ é um corpo e portanto todo elemento não nulo é invertível, consequentemente

$$\Phi(\pi) = N(\pi) - 1$$

Seja $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$. Um conjunto $\{\beta_1, \dots, \beta_{\Phi(\alpha)}\} \subset \mathbb{Z}[i]$

é um sistema reduzido de resíduos módulo α , se

$$(\mathbb{Z}[i]/I(\alpha))^* = \{\bar{\beta}_1, \dots, \bar{\beta}_{\Phi(\alpha)}\}.$$

Note que um subconjunto Λ de $\mathbb{Z}[i]$ é um sistema reduzido de resíduos módulo α se e somente se, são simultaneamente verificadas as condições,

- (i) Λ tem $\Phi(\alpha)$ elementos,
- (ii) As classes residuais em $\mathbb{Z}[i] / I(\alpha)$ dos elementos de Λ são duas a duas distintas,
- (iii) As classes residuais dos elementos de Λ são invertíveis em $\mathbb{Z}[i]/I(\alpha)$.

(A verificação da afirmação é simples e a deixamos como exercício).

O seguinte resultado é análogo ao Teorema de Euler (veja Problema 2.5, Capítulo 6).

Teorema 5 (Gauss). *Sejam $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$ e $\beta \in \mathbb{Z}[i]$ tais que $(\beta, \alpha) = 1$. Temos então em $\mathbb{Z}[i]/I(\alpha)$ a seguinte igualdade,*

$$(\bar{\beta})^{\Phi(\alpha)} = \bar{1}$$

Demonstração: Seja $\{\beta_1, \dots, \beta_{\Phi(\alpha)}\}$ um sistema reduzido de resíduos módulo α . Sendo $(\beta, \alpha) = 1$, tem-se que $\{\beta \cdot \beta_1, \dots, \beta \cdot \beta_{\Phi(\alpha)}\}$ é um sistema reduzido de resíduo módulo α (veja Problema 4.3). Temos então em $\mathbb{Z}[i]/I(\alpha)$ que

$$(\bar{\beta})^{\Phi(\alpha)} \cdot \bar{\beta}_1 \cdots \bar{\beta}_{\Phi(\alpha)} = \bar{\beta}_1 \cdots \bar{\beta}_{\Phi(\alpha)}.$$

Como $\bar{\beta}_1, \dots, \bar{\beta}_{\Phi(\alpha)}$ são invertíveis em $\mathbb{Z}[i]/I(\alpha)$, o resultado segue da igualdade acima. \square

Os próximos resultados nos permitirão calcular explicitamente o valor de $\Phi(\alpha)$, para $\alpha \in \mathbb{Z}[i]$.

Proposição 7. *Sejam π um elemento primo de $\mathbb{Z}[i]$ e $n \in \mathbb{N}$. Temos que*

$$\Phi(\pi^n) = N(\pi^n) \left(1 - \frac{1}{N(\pi)}\right).$$

Demonstração: Seja $\{\alpha_1, \dots, \alpha_{N(\pi^n)}\}$ um sistema completo de resíduos módulo π^n . Isto é, elementos de $\mathbb{Z}[i]$ dois a dois incongruentes módulo π^n e cujas classes residuais nos dão todas as classes de $\mathbb{Z}[i]/I(\pi^n)$. Sejam $\alpha_{\ell_1}, \dots, \alpha_{\ell_r}$ os elementos do conjunto acima cujas classes residuais são não invertíveis em $\mathbb{Z}[i]/I(\pi^n)$. Temos então que $\pi | \alpha_{\ell_j}$ para todo j e que

$$\left\{ \frac{\alpha_{\ell_1}}{\pi}, \dots, \frac{\alpha_{\ell_r}}{\pi} \right\}$$

forma um sistema completo de resíduos módulo π^{n-1} . Temos então que $r = N(\pi^{n-1})$ e consequentemente,

$$\Phi(\pi^n) = N(\pi^n) - N(\pi^{n-1}) = N(\pi^n) \left(1 - \frac{1}{N(\pi)} \right). \quad \square$$

Teorema 6. Seja $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$ com decomposição em fatores primos,

$$\alpha = \pi_1^{n_1} \cdots \pi_r^{n_r}$$

Temos então que

$$\Phi(\alpha) = N(\alpha) \left(1 - \frac{1}{N(\pi_1)} \right) \cdots \left(1 - \frac{1}{N(\pi_r)} \right).$$

Demonstração: Como $(\pi_j, \pi_\ell) = 1$ para $j \neq \ell$, temos, pelo Corolário 2 do Teorema 1 do Capítulo 7, um isomorfismo de anéis

$$\mathbb{Z}[i]/I(\alpha) \simeq \mathbb{Z}[i]/I(\pi_1^{n_1}) \times \cdots \times \mathbb{Z}[i]/I(\pi_r^{n_r}).$$

Pela Proposição 5 do Capítulo 7 segue que

$$(\mathbb{Z}[i]/I(\alpha))^* = (\mathbb{Z}[i]/I(\pi_1^{n_1}))^* \times \cdots \times (\mathbb{Z}[i]/I(\pi_r^{n_r}))^*,$$

logo

$$\Phi(\alpha) = \Phi(\pi_1^{n_1}) \cdots \Phi(\pi_r^{n_r}),$$

que pela Proposição 7 nos dá

$$\begin{aligned} \Phi(\alpha) &= N(\pi_1^{n_1}) \cdots N(\pi_r^{n_r}) \left(1 - \frac{1}{N(\pi_1)} \right) \cdots \left(1 - \frac{1}{N(\pi_r)} \right) \\ &= N(\alpha) \left(1 - \frac{1}{N(\pi_1)} \right) \cdots \left(1 - \frac{1}{N(\pi_r)} \right). \end{aligned} \quad \square$$

Problemas

4.1 Seja $\alpha = 12 + 6i$. Determine o número de elemento de $\mathbb{Z}[i]/I(\alpha)$ e descreva um sistema completo de resíduos módulo α .

4.2 Ache todos os elementos invertíveis de $\mathbb{Z}[i]/I(3 + 6i)$.

4.3 Seja $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$. Mostre que se $\{\beta_1, \dots, \beta_{\Phi(\alpha)}\}$ é um sistema reduzido de resíduos módulo α e se $\beta \in \mathbb{Z}[i]$ é tal que $(\beta, \alpha) = 1$, então $\{\beta \cdot \beta_1, \dots, \beta \cdot \beta_{\Phi(\alpha)}\}$ é um sistema reduzido de resíduos módulo α .

4.4 Seja π um elemento primo de $\mathbb{Z}[i]$. Mostre que para todo $\beta \in \mathbb{Z}[i]$ temos em $\mathbb{Z}[i]/I(\pi)$, que

$$(\overline{\beta})^{N(\pi)} = \overline{\beta}.$$

4.5 Seja $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$ e seja $\{\beta_1, \dots, \beta_{\Phi(\alpha)}\}$ um sistema reduzido de resíduos módulo α .

a) Mostre que em $\mathbb{Z}[i]/I(\alpha)$ vale a igualdade,

$$\overline{\beta}_1 \cdots \overline{\beta}_{\Phi(\alpha)} = \overline{-1}$$

b) Suponha que α seja um primo da forma $a + bi$ com $a \cdot b \neq 0$. Mostre que em $\mathbb{Z}[i]/I(\alpha)$ vale a seguinte igualdade análoga à do Teorema de Wilson,

$$\overline{(N(\alpha) - 1)!} = \overline{-1}$$

4.6 Calcule

- | | | |
|-------------------|--------------------|---|
| a) $\Phi(7)$ | b) $\Phi(5)$ | c) $\Phi(1 + i)$ |
| d) $\Phi(2 + 3i)$ | e) $\Phi(12 + 6i)$ | f) $\Phi(2^r)$ com $r \in \mathbb{N}$. |

4.7 Seja $\alpha = d(a + bi)$ com $d \in \mathbb{N}$, $a + bi \in \mathbb{Z}[i]$ e $(a, b) = 1$. Mostre que o núcleo do homomorfismo característico ρ de \mathbb{Z} em $\mathbb{Z}[i]/I(\alpha)$ é gerado por $d(a^2 + b^2)$.

4.8 Determine a característica de $\mathbb{Z}[i]/I(\alpha)$, onde

- | | | | |
|----------------------------|---------------------|---------------------|----------------------|
| a) $\alpha \in \mathbb{Z}$ | b) $\alpha = 1 + i$ | c) $\alpha = 2 + i$ | d) $\alpha = 6 + 3i$ |
|----------------------------|---------------------|---------------------|----------------------|

Sugestão: Utilize o problema anterior.

5. O Exemplo de Kummer

Para produzir um exemplo de domínio de integridade onde os conceitos de elementos primos e irredutíveis não coincidem, Kummer considerou o subanel $\mathbb{Z}[\sqrt{5}i]$ de \mathbb{C} gerado por \mathbb{Z} e por $\sqrt{5}i$. É este anel que estudaremos a seguir.

Proposição 8. *Temos que $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$.*

Demonstração: Como temos as inclusões

$$\mathbb{Z} \cup \{\sqrt{5}i\} \subset \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{5}i],$$

e como $\mathbb{Z}[\sqrt{5}i]$ é o menor subanel de \mathbb{C} que contém \mathbb{Z} e $\sqrt{5}i$, para provar o resultado basta mostrarmos que $\{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ é um subanel de \mathbb{C} .

De fato, note que

$$1 = 1 + 0\sqrt{5}i \in \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\},$$

e que se $z = a + b\sqrt{5}i$ e $z' = a' + b'\sqrt{5}i$ são elementos de $\{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$, então

$$z - z' = (a - a') + (b - b')\sqrt{5}i$$

e

$$z \cdot z' = (a' - 5bb') + (ab' + a'b)\sqrt{5}i$$

são elementos de $\{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$. O resultado segue da Proposição 1 do Capítulo 7. \square

Os elementos invertíveis de $\mathbb{Z}[\sqrt{5}i]$ são caracterizados a seguir.

Proposição 9. *Seja $\alpha \in \mathbb{Z}[\sqrt{5}i]$. Então as seguintes afirmações são equivalentes.*

- (i) α é invertível em $\mathbb{Z}[\sqrt{5}i]$;
- (ii) $N(\alpha) = 1$;
- (iii) $\alpha \in \{-1, 1\}$.

Demonstração: A demonstração é semelhante à da Proposição 2 e a deixamos como exercício. \square

A seguir daremos uma caracterização dos elementos irreduutíveis de $\mathbb{Z}[\sqrt{5}i]$.

Teorema 7. Seja $\alpha = a + b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$. Tem-se que α é irreduutível em $\mathbb{Z}[\sqrt{5}i]$ se a equação diofantina,

$$x^2 + 5y^2 = d,$$

não admite solução para todo divisor positivo próprio d de $a^2 + 5b^2$ em \mathbb{Z} .

Demonstração: Provaremos que se α é redutível então a equação diofantina acima admite solução para todo divisor próprio d de $a^2 + 5b^2$ em \mathbb{N} .

Suponha que $\alpha = a + b\sqrt{5}i$ seja redutível, logo

$$\alpha = (u + v\sqrt{5}i)(u' + v'\sqrt{5}i)$$

com $u + v\sqrt{5}i$ e $u' + v'\sqrt{5}i$ não invertíveis e portanto pela Proposição 9 com $N(u + v\sqrt{5}i) \neq 1$ e $N(u' + v'\sqrt{5}i) \neq 1$. Segue então que

$$a^2 + 5b^2 = N(\alpha) = N(u + v\sqrt{5}i) \cdot N(u' + v'\sqrt{5}i) = (u^2 + 5v^2) \cdot d',$$

onde $d' = u'^2 + 5v'^2$. Temos então que $x = u$ e $y = v$ é uma solução da equação

$$x^2 + 5y^2 = d,$$

onde $d = \frac{a^2 + 5b^2}{d'} \in \mathbb{N}$ é um divisor próprio de $a^2 + 5b^2$. □

Exemplos

1. 2 é irreduutível em $\mathbb{Z}[\sqrt{5}i]$ pois a equação diofantina

$$x^2 + 5y^2 = d$$

para d divisor próprio de 4 não admite soluções em \mathbb{Z} .

2. 3 é irreduutível em $\mathbb{Z}[\sqrt{5}i]$ pois a equação diofantina

$$x^2 + 5y^2 = d$$

para d divisor próprio de 9 não admite soluções em \mathbb{Z} .

3. $1 \pm \sqrt{5}i$ são irreduutíveis em $\mathbb{Z}[\sqrt{5}i]$ pois a equação diofantina

$$x^2 + 5y^2 = d$$

para d divisor próprio de 6 não admite soluções em \mathbb{Z} .

Note agora que $2 | (1 + i\sqrt{5})(1 - i\sqrt{5})$ e no entanto $2 \nmid (1 + i\sqrt{5})$ e $2 \nmid (1 - i\sqrt{5})$. Portanto 2 é irreduutível mas não é primo em $\mathbb{Z}[\sqrt{5}i]$. Este fato implica que $\mathbb{Z}[\sqrt{5}i]$ não é Domínio de Fatoração Única. A título de exemplo damos duas fatorações distintas de um elemento de $\mathbb{Z}[\sqrt{5}i]$:

$$6 = 2 \times 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

Problemas

5.1 Seja $\alpha \in \mathbb{Z}[\sqrt{5}i]$

- a) Mostre que se α é primo em $\mathbb{Z}[\sqrt{5}i]$ então α divide um número primo p de \mathbb{Z} ;
- b) Mostre que há dois tipos de elementos primos de $\mathbb{Z}[\sqrt{5}i]$, os primos p de \mathbb{Z} para os quais a equação diofantina $x^2 + 5y^2 = p$ não tem soluções em \mathbb{Z} e os elementos $\alpha \in \mathbb{Z}[\sqrt{5}i]$ tais que $\alpha\bar{\alpha}$ é um primo de \mathbb{Z} .

5.2 Considere o subanel $\mathbb{Z}[\sqrt{2}]$ de \mathbb{R} .

- a) Mostre que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$;
- b) Considere a função norma definida em $\mathbb{Z}[\sqrt{2}]$

$$N(a + b\sqrt{2}) = |(a + b\sqrt{2})(a - b\sqrt{2})| = |a^2 - 2b^2|.$$

Mostre que

$$N((a + b\sqrt{2}) \cdot (a' + b'\sqrt{2})) = N(a + b\sqrt{2}) \cdot N(a' + b'\sqrt{2}).$$

Mostre que $a + b\sqrt{2}$ é invertível em $\mathbb{Z}[\sqrt{2}]$ se e somente se $N(a + b\sqrt{2}) = |a^2 - 2b^2| = 1$.

Mostre que $(1 - \sqrt{2})^n$ é invertível em $\mathbb{Z}[\sqrt{2}]$ para todo $n \in \mathbb{Z}$.

- c) Mostre que em $\mathbb{Z}[\sqrt{2}]$ tem-se uma divisão com resto pequeno, isto é, dados $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ com $\beta \neq 0$, existem $q, r \in \mathbb{Z}[\sqrt{2}]$ tais que

$$\alpha = \beta \cdot q + r \quad \text{com} \quad N(r) < N(\beta).$$

Bibliografia

- [1] W.J. Leveque, *Topics in Number Theory, Volume 1*, Addison-Wesley 1956.
- [2] L.H.J. Monteiro, *Elementos de Álgebra*, Coleção Elementos de Matemática, Ao Livro Técnico 1969.
- [3] I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley 1966.
- [4] S. Sidki, *Introdução à Teoria dos Números*, 10º Colóquio Brasileiro de Matemática, IMPA 1975.
- [5] A. Weil, *Number Theory for Beginners*, com a colaboração de M. Rosenlicht, Springer-Verlag 1979.

Índice

A

- Adição 23
- Algoritmo de Euclides 95
- Anel
 - Anel 23, 132
 - ordenado 27
 - quociente 141
- Associado 68

B

- Binômio de Newton 50

C

- Característica 144
- Classe de equivalência 36
- Classe residual 116
- Coleção 1
- Congruência 107
- Congruência linear 123
- Conjugação 184
- Conjunto
 - das partes 9
 - finito 44
 - infinito 44
 - limitado inferiormente 29
 - limitado superiormente 29
 - vazio 5
- Corpo
 - arquimediano 154
 - completo 170
 - de frações 35

- dos números complexos 178
- dos números racionais 37
- dos números reais 165
- ordenado 40
- Critérios de divisibilidade 109, 110, 111
- Crivo de Eratóstenes 88

D

- Desigualdade de Bernoulli 53
- Diferença de conjuntos 8
- Dividendo 57
- Divisão Euclidiana 56
- Divisibilidade 66
- Divisor 57, 66
- Domínio
 - bem ordenado 30
 - de fatoração única 79
 - de integridade 25
 - ordenado 27
 - principal 75

E

- Elemento
 - invertível 25
 - irredutível 77
 - primo 79
 - redutível 77
 - unidade 24
- Equação
 - diofantina 101
 - pitagórica 210

Exemplo de Kummer 218
Expansão b-ádica 61
Extensão de corpos 134

F

Famílias de conjunto 10
Fatorial 46
Forma trigonométrica 186
Fórmula de De Moivre 188
Função
 função 12
 bijetora 18
 composta 15
 Φ de Euler 121, 127, 146
 Φ de Gauss 214
 identidade 13
 injetora 17
 norma 199
 parte inteira 57
 sobrejetora 18

H

Homomorfismo 31, 136
Homomorfismo característico 48

I

Ideal
 ideal 72, 136
 maximal 138
 primo 138
Imagem direta 16
Imagem inversa 16
Indeterminada 3
Inteiros Gaussianos 189
Interseção de conjuntos 7
Isomorfismo 32

M

Maior elemento 29
Máximo divisor comum 68
Menor elemento 29
Mínimo múltiplo comum 70

Módulo 184
Multiplicação 23
Múltiplo 66

N

Número
 complexo 177
 de Fermat 91
 de Mersenne 91
 inteiro 2, 23
 natural 2
 racional 35
 real 148

P

Pequeno Teorema de Fermat 92, 114
Postulado de Bertrand 93
Princípio
 das gavetas 45
 de Boa Ordenação 30
 de Dirichlet 45
 de indução matemática 42
 do supremo 173
Produto cartesiano 10
Progressão Aritmética 54
Progressão Geométrica 55
Propriedade Arquimediana 31
Prova dos nove 110

Q

Quociente 57

R

Raíz da unidade 192
Raíz primitiva da unidade 194
Relação binária 27
Relação de equivalência 36
Relação de Stifel 51
Representante 36
Resto 57
Restrição 14

S

Sentença aberta 3
Seqüênciaseqüência 13
convergente 149
de Cauchy 159
divergente 150
fundamental 159
limitada 150, 151
nula 150
Subanel 32, 132
Subtração 25
Série 158
Série geométrica 158
Subcorpo 134

T

Teorema
de Dirichlet 95

de Fermat 207, 209
de Gauss 215
de Wilson 122
do isomorfismo 142
dos Números Primos 94
Fundamental da Aritmética 83

U

Último Teorema de Fermat 104,
105

União de conjuntos 6

V

Valor absoluto 27
Valor absoluto p -ádico 86